Anna van Buerenplein 1
2595 DA Den Haag
P.O. Box 96800
2509 JE The Hague
The Netherlands

www.tno.nl

T +31 88 866 00 00

TNO report

TNO 2022 R10507

Bridging the Dutch and European Digital Sovereignty gap

Date	March 21 2022
Author(s)	Claire Stolwijk, Matthijs Punter, Tjerk Timan, Frank Berkers, Ilina Georgieva, Rick Gilsing, Harrie Bastiaansen, Marissa Hoekstra, Anastasia Yagafarova, Wico Mulder, Simon Dalmolen, Rieks Joosten
Number of pages	82
Number of appendices	8
Project name	Digital Sovereignty
Project number	060.49495

Acknowledgement

We want to thank the following experts for their input: Henk Jan Vink, Berry Vetjens, Freek Bomhof, Thijmen van Bree, Marcel de Heide, Ton van Mol, Pieter Nooren, Toon Norp, Elmer Rietveld, Rogier Verberk, Jesse Robbers, Mike de Roode.

Table of contents

Abstract

"Now is the time for Europe to be digitally sovereign," German Chancellor Angela Merkel, Danish Prime Minister Mette Frederiksen, Estonian Prime Minister Kaja Kallas, and Finnish Prime Minister Sanna Marin said this in a joint letter[1] because:

- 92% of data from the West is hosted in the US and only 4% is stored in Europe.[2]
- The core of the digital infrastructure is provided by non-European suppliers (e.g. for routers, switches, encryptors and servers).[3]
- There are no European companies in the Top 20 of global tech brands.

At least four nations from the EU want to become digital sovereign since it has become a concern for policymakers who feel too much power is in the hands of a small number of large tech companies.[4] This results in a strong digital dependence, which means a lack of competition which could adversely affect the setting of fair prices and the quality of products, as well as innovation.[5] The COVID19 pandemic, which made us more dependent on digital technologies, has stimulated the debate on digital sovereignty in the Netherlands and in Europe; digital sovereignty has recently been placed on the political agenda, and can be defined as: *"control over the design and use of (business) critical digital systems, algorithms and the data generated and processed with them".*[6]

In the digital domain, Europe is primarily focusing on regulatory power, in its most explicit form through for instance the General Data Protection Regulation (GDPR), the Data Governance Act., and the Digital Services Act (DSA). The American sometimes say about this: *'the US innovates, Europe regulates'.*[7] Europe claims moral and legal authority, in which, for example, privacy is regarded as a collective fundamental right and not as something that can be arranged between the individual consumer and service provider through conditions and settings.[8] The chairman of the European Commission von der Leyen has commented on this and said; *"you must not only regulate, but also have the technology to anchor your own values*".[9] However, this involves a balancing act when achieving a certain degree of autonomy and self-reliance without pursuing protectionist policies.

In general, there is a lot of unclarity about digital sovereignty, and a clear multidisciplinary overview to enable digital sovereignty is currently lacking. Questions such as: 'what measures are currently in place and which measures are still missing', are pressing yet remain unanswered. In this paper, we will answer these questions. We also focus on the role that applied research can fulfil to improve digital sovereignty for the Netherlands and Europe.

---

[1] Who owns data and who controls it? | World Economic Forum (weforum.org)
[2] https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf
[3] Based on expert input.
[4] Ontwakende Europese digitale soevereiniteit | iBestuur
[5] https://www.lecese.fr/sites/default/files/travaux_multilingue/2019_07_souverainete_europeenne_numerique_GB_reduit.pdf#page8
[6] Based on https://www.uu.nl/sites/default/files/Moerel%2C%20Timmers%20%282.0%29%20-%20Preadvies%20Staatsrechtconferentie%202020.pdf
[7] https://ibestuur.nl/podium/ontwakende-europese-digitale-soevereiniteit
[8] Ibid
[9] Ibid

1. Introduction

1.1 Why this topic

Society and economy are increasingly dependent on ICT and connectivity. This became especially clear during the COVID19 pandemic, where digital means enabled many people to telework from home.[10] Teleworking saved many sectors in the economy from collapse, resulting also in diverting a larger economic disruption. Digitalisation also improved value chain cooperation for various sectors, making value chains more transparent and resilient; in its wake also turning many such value chains into value networks.

Besides such benefits, digitalisation also comes with disadvantages. It has made societies more vulnerable for cyber threats and it has made them more dependent on digital technologies that are often in the hands of a limited number of foreign players.[11] This dependency accelerated the political discussion on digital sovereignty both on national as well as on European level. [12] While such political agenda-setting is crucial, the topic is rarely analysed in detail and often from singular perspectives (e.g. policy perspective only, or technological perspective only), with a growing number of exceptions (examples of more extensive scientific investigations are; Couture & Toupin, 2019; Mueller, 2010, 2019; Pohle, 2020c; Pohle & Thiel, 2019; Thiel, 2014, 2019; Glasze & Dammann, in press; Peuker, 2020[13]). Therefore in this paper we analyse digital sovereignty from different perspectives (e.g. policy and technological, but also from economic-, innovation-, societal- and geopolitical perspectives).

1.2 Definition of the topic

Sovereignty is often associated with territoriality, territory, jurisdiction, a population, autonomy, authority with internal recognition and external recognition. Digital sovereignty focuses on the digital dimension and is in this paper defined as: *"control over the design and use of (business) critical digital systems, algorithms and the data generated and processed with them".*[14]

Various experts indicated that there is a so-called digital sovereignty gap both on national as well as on European level. They say: *"The EU has the ambition and potential to become a sovereign digital power, but it lacks an all-encompassing strategy, in which individual governments are the key players".*[15] They also mention: *"Achieving this will involve creating legal, regulatory, and financial instruments that can help the EU actively promote European values and principles in this domain. Without its own digital capacities and autonomy, Europe will not be able to fully*

[10] jrc120945_policy_brief_-_covid_and_telework_final.pdf (europa.eu)
[11] WRR Advies Digitale Ontwrichting, https://www.wrr.nl/adviesprojecten/digitale-ontwrichting.
[12]https://www.cybersecuritycouncil.nl/documents/reports/2021/02/17/report-strategic-autonomy-and-cybersecurity-in-the-netherlands
[13] https://policyreview.info/concepts/digital-sovereignty
[14] Based on https://www.uu.nl/sites/default/files/Moerel%2C%20Timmers%20%282.0%29%20-%20Preadvies%20Staatsrechtconferentie%202020.pdf
[15] https://ecfr.eu/publication/network-effects-europes-digital-sovereignty-in-the-mediterranean/

contend with other actors in the tech space and will find itself caught up in rising US-China competition for technological supremacy".
However, closing this digital sovereignty gap involves a difficult balancing act.[16] The aim is to avoid that Europe becomes too dependent on foreign players for their safety and health.[17] On the other hand, policymakers often do not want to pursue protectionist policies that favour their own industry and exclude foreign players.[18] Europe stands for an open economy and free trade, based on reciprocity.

1.3 Goal and target group of the paper

To goal of this paper is to:

- Clarify the topic digital sovereignty to policy makers and stakeholders involved in various sectors (e.g. smart production, smart agro food etc.) from different perspectives (e.g. policy and technological, but also the economic, innovation, societal and geopolitical perspectives).
- Provide an overview of the state of play of the measures to stimulate digital sovereignty.
- Indicate what additional measures could be applied based on the preferred scenario of digital sovereignty**.**

1.4 Reading guide

- In Chapter 2 we describe the state of play of the current digital sovereignty based on different digital technology layers and boundary conditions.
- Chapter 3 describes the role of digital sovereignty in promising innovation areas in several domains (e.g. Smart Health, Smart Mobility etc).
- In Chapter 4 four scenarios are presented about the future digital sovereignty, including the current and preferred scenario.
- Chapter 5 presents the key issues that needs to be solved to go from the current towards the preferred scenario.
- Chapter 6 describes the measures to solve the key issue to come to the preferred scenario.
- In Chapter 7 we end the paper with the concluding summary.

[16] Hoe vult Europa het verlangen naar technologische soevereiniteit in? | Rathenau Instituut (in Dutch)
[17] Ibid
[18] Ibid

2. The state of play

2.1 Technology level model

The Netherlands and Europe currently have insufficient insight into new dependencies for their digital technologies on foreign countries. That is why they are not able to pursue sufficiently proactive coordinated policy solutions.[19] The new technologies are so interwoven that with for instance a one-sided focus on cyber resilience, the greater implications for digital sovereignty will be missed.[20]

In this section we introduce a technology level model to provide more insights in the dependence of the Netherlands and Europe on foreign countries. Our technology level model contains four components.

1. Digital technology layers (in the middle of Figure 1)
   Digital technologies are increasingly pervasive. They are no longer limited to mainframes and personal computers, instead they are part of most physical assets and services. In addition technologies are increasingly intertwined to provide an integrated end-user experience. In the context of this paper we distinguish between several technology layers:

- **Networks and connectivity**: infrastructures to exchange data between systems, e.g. 5G wireless networks and next generation high-bandwidth fixed connections.
- **Data storage and cloud**: infrastructures to store data, sometimes locally, sometimes in shared data centres, which should seamlessly work together.
- **Information & data infrastructures**: software components responsible for the capturing, basic processing and controlled sharing of data both within an organization and between multiple parties in a data space.
- **Algorithms**: approaches for machine learning and other aspects of artificial intelligence for the analysis and interpretation of data.
- **Applications:** end-user applications and graphical user interfaces building on this technology stack.

2. Influencing factors (at the bottom of Figure 1)
   Influencing factors such as materials and components are highly influencing the digital sovereignty, therefore we also incorporated those in our model.
   - **Material availability and sourcing**: materials need to be available to produce the required digital components. These relate to both raw materials (e.g. to produce batteries) and components (e.g. microchips).

3. Potential disrupting factors (at the left and right of Figure 1)
   Technologies will evolve as time passes, with incremental innovations. There are however also some disruptors, which might fundamentally shift these developments. For digital technologies there are several areas where potential disruptions can come from, who are able to change the current digital sovereignty status, in particular:

[19] https://www.uu.nl/sites/default/files/Moerel%2C%20Timmers%20%282.0%29%20-%20Preadvies%20Staatsrechtconferentie%202020.pdf
[20] Ibid

- **Smaller, cheaper and more powerful hardware**: if technologies become smaller and more energy-efficient, this will enable technologies to be embedded in many more systems and services. This will also enable more distributed approaches for data access and processes. This potential disruptor also includes new antennas/communication technologies and new battery technologies, which both can enable digital technologies to become more pervasive.
- **New paradigms for cryptography & quantum technology**: current digital technologies are all based on computing principles dating back to the previous century. New paradigms, mostly under the umbrella of quantum technology (e.g. quantum computing), can have a significant impact. For instance to provide new approaches for cryptography and resulting security.

4. Boundary condition factors (at the top of Figure 1)
   Two types of boundary conditions that can strengthen the sovereignty of the aforementioned layers of the technology level model are:
   - **Policies:** show which policy instruments are needed to stimulate digital technologies and the related sovereignty.
   - **Business models**: indicate under which conditions technologies are being developed and brought to the market.

Combined this results in the following model (see Figure 1):

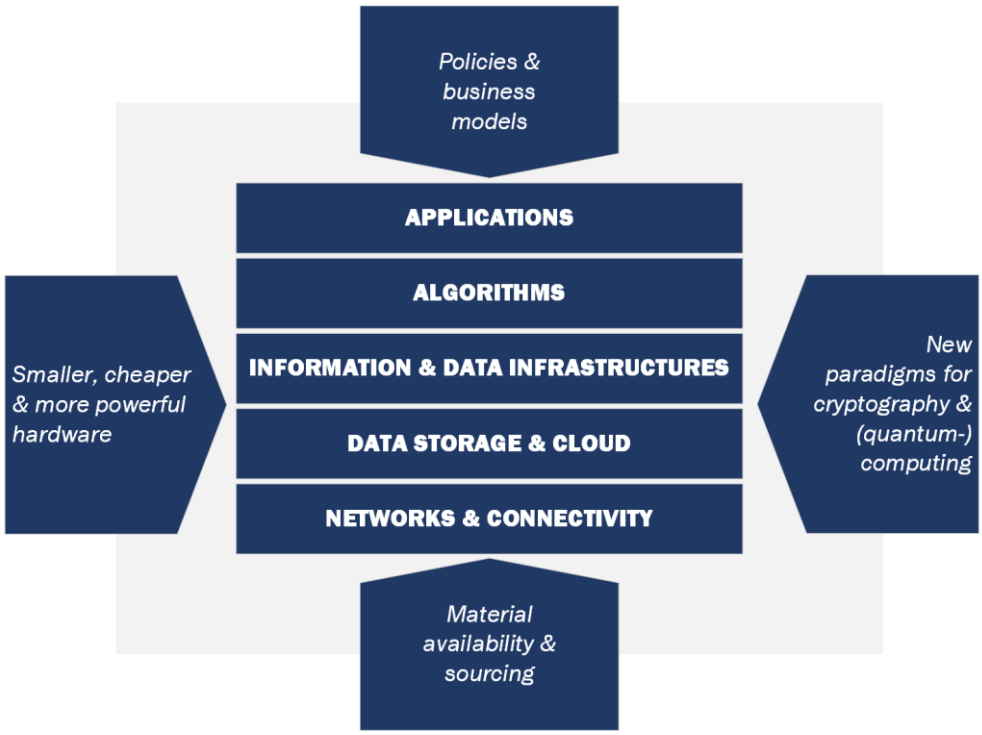


Figure 1. Technology level model

2.2 Digital technology layers

In this section each technology layer will be described and the digital sovereignty on each digital technology layer will be elaborated.

2.2.1 Networks & connectivity

Networks and connectivity is the first digital technology layer of the technology level model and concerns infrastructures to exchange data between systems such as 5G, 6G (and beyond), wireless networks and the next generation high-bandwidth fixed connections.[21]

While Europe was well positioned in the specifications of international standards for 2G, 3G and 4G cellular networks, the situation has shifted regarding 5G.[22] The question is who will be leading 5G in the next years?[23] Can Europe become leading in this area? This seems challenging:

- Huawei is currently the global market leader of 5G, while Ericsson and Nokia offer a European alternative.[24]
- 5G is the subject of geo-political discussions between the US and China. Discussions relate to security concerns with Chinese equipment.
- Europe has the lowest number of 5G base stations per million inhabitants (7) compared to China (94) or the US (31). [25]
- Each of these 5G network vendors use proprietary interfaces. This generates undesirable lock-in effects, holds back innovation and reduces flexibility in terms of switching to current and future standards (5G, 6G). [26]

Therefore beyond 5G, the European Commission now intends to focus on the next development towards 6G.[27] 6G could become an enabler for the digital society, where all kinds of applications as healthcare (healthcare will become AI-driven and dependent on 6G communication technology[28]), transport (e.g. communication for Connected Cars and Autonomous Driving[29]), and Industry 4.0 (enabler for Industrial Internet of Everything) depend on 6G networks.[30]

2.2.2 Data storage & cloud

Data storage and cloud is the second digital technology layer of the technology level model and can be defined as infrastructures to store data, sometimes locally, sometimes federated, but often in shared data centres using proprietary technologies (e.g. provided by Big Tech).
Similar to networks and connectivity this second layer also contains a strong non-European dependency, since there are currently no European firms within the top 5

[21] https://www.researchgate.net/publication/347799507_Towards_6G_wireless_communication_networks_vision_enabling_technologies_and_new_paradigm_shifts/link/5ff972d592851c13fefb4189/download
[22] https://www.coursehero.com/file/p6t73o7e/Chinese-companies-are-also-increasingly-active-in-international-standard/
[23] https://itif.org/publications/2020/11/30/great-5g-race-china-really-beating-united-states
[24] Acatech. Digital Sovereignty. Status Quo and Perspectives.
[25] https://www.oliverwyman.com/our-expertise/insights/2020/sep/european-digital-sovereignty.html
[26] Acatech. Digital Sovereignty. Status Quo and Perspectives. https://en.acatech.de/publication/digital-sovereignty/
[27] Ibid
[28] https://arxiv.org/abs/2005.07532
[29] https://grapeup.com/blog/the-future-of-autonomous-driving-connectivity-quantum-entanglement-or-6g/
[30] 6G Opportunities Arising from Internet of Things Use Cases: A Review Paper: https://www.mdpi.com/1999-5903/13/6/159

of cloud providers. [31] The European Gaia-X[32] initiative aims to build a network of providers who develop and provide federated infrastructure services (IaaS/CaaS/PaaS) using precisely defined common standards, free software and documented operating processes. The diversity of providers (and the option for companies to run their own environments) will create an interoperable virtual cloud. Even though Gaia-X is not mature yet, it has strong backing from the German government which has also reached out to France in the first place and connected later to other countries in Europe as well, the Netherlands being one of them. At this point in time, both Gaia-X and International Data Spaces Association (IDSA)[33] (for more details on the IDSA see Appendix B, for more details on data spaces see section 2.2.3) seem to be best placed to deliver the standards needed for interoperability. At the same time, it is important to keep our eyes open for comparable alternatives that may gain traction, given the fact that both Gaia-X and IDSA are still under development.

For the time being, large cloud providers (e.g. Google, Amazon) that dominate the cloud and expand their business into numerous related verticals, cannot be rapidly replaced in Europe, even if Gaia-X is successfully implemented. They are often called hyperscalers.[34] Besides that, the fact that the American hyperscalers are governed by the US CLOUD Act threatens the security of data stored in Europe. The dependencies are however not necessarily the same across all segments of the cloud market and computing continuum.[35] In particular, EU industry is for now less dependent in the nascent edge computing segment, certain market subsegments of the cloud service offerings and in the system integration of smart and low power cloud platforms and middleware.[36,37]

Data storage and cloud are important for almost every domain and application area we can imagine. That is why an initiative such as Gaia-X is focusing on various application areas such as agriculture, education and skills, energy, finance, geoinformation, health, industry 4.0, mobility, public sector and smart living. The solution in following the European Values regarding data sharing and AI and being sovereign is introducing portability and interoperability:

- Gaia-X Portability of data and services: Data is described in a standardised protocol that enables transfer and processing to increase its usefulness as a strategic resource. Services can be migrated without significant changes and adaptations and have a similar quality of service (QoS) as well as the same Compliance level.

[31] https://www.oliverwyman.com/our-expertise/insights/2020/sep/european-digital-sovereignty.html
[32] https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html
[33] https://internationaldataspaces.org/
[34] https://www.digitalrealty.com/blog/what-is-hyperscale
[35] Acatech. Digital Sovereignty. Status Quo and Perspectives. https://en.acatech.de/publication/digital-sovereignty/
[36] Acatech. Digital Sovereignty. Status Quo and Perspectives. https://en.acatech.de/publication/digital-sovereignty/
[37] Commission staff working document. Strategic dependencies and capacities accompanying the Communication from the Commission to the European Parliament, the Council, the European and Economic and Social Committee and the Committee of the Regions. Updating the 2020 New Industrial Strategy: Building a stronger Single Market for Europe's recovery. (2020). swd-strategic-dependencies-capacities_en.pdf (europa.eu)

- Gaia-X Interoperability of data and services: The ability of several systems or services to exchange information and to use the exchanged information in mutually beneficial ways.

2.2.3 Information & data sharing infrastructures

The third digital technology layer, Information and data sharing infrastructures, concern software components responsible for the capturing, basic processing and controlled sharing of data both within and between multiple parties in a data space. This layer can be seen as an orchestration layer. This is also an area which the Gaia-X initiative aims to address.

Just like the data storage and cloud layer, the layer of information and data infrastructures is currently driven by hyperscalers, providing an integrated cloud-data sharing offering. It is the basis for many end-user data sharing applications. [38] To reduce dependency on non-European countries, the European Commission has released publications on the European Data Strategy[39] and the Data Governance Act.[40] Moreover, its release of the Data Governance Act and the additional input sought on European data spaces through OPEN DEI[41, 42] point to the importance that the EU attributes to data spaces and data sharing alternatives for the hyperscalers. OPEN DEI *has defined a data space as a 'decentralised infrastructure for trustworthy data sharing and exchange in data ecosystems based on commonly agreed principles',* so that participants can retain absolute control and transparency over what happens with their data. Furthermore, "security-by-design" helps participants to become more sovereign. For example, to have the option to revoke consent. In its work on data space design principles, the EU OPEN DEI initiative distinguishes three types of building blocks:

1. *Data platforms*, providing support for effective data sharing and exchange as well as for engineering and deployment of data exchange and processing capabilities;
2. *Data marketplaces*, where data providers can offer and data consumers can request data[43], as well as data processing applications;
3. *Blocks ensuring data sovereignty*, i.e. the ability for each stakeholder to control their data by making decisions as to how digital processes, infrastructures, and flows of data are structured, built and managed, based on an appropriate governance scheme enabling specification of terms and conditions.

The infrastructure based on these three building blocks is referred to as a 'soft infrastructure'. In a federation of data spaces, each individual data space instance has a high degree of autonomy in developing and deploying its own internal agreements and ICT landscape. However, jointly the individual data space instances pursue a common goal of being able to share data in a trusted manner.

Currently, a multitude of data sharing domains have been developed for various sectors and application areas, varying in the level of being in accordance with the

[38] Acatech. Digital Sovereignty. Status Quo and Perspectives. https://en.acatech.de/publication/digital-sovereignty/

[39] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN.

[40] https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767.

[41] Aligning Reference Architectures, Open Platforms and Large-Scale Pilots in Digitising European Industry

[42] EU OPEN DEI Initiative. "Design Principles for data spaces – Position Paper". Version 1.0. April 2021, https://design-principles-for-data-spaces.org/.

[43] Note: data marketplaces only aggregate metadata and do not store the actual data

data space definition and principles and with varying usage scenarios. To illustrate the potential of the federated and interoperable data space approach, the International Data Spaces Association (IDSA) has provided an overview of use cases.[44] These use cases are illustrative and representative for a much broader set of use cases. For the federation of data spaces to seamlessly interconnect, interoperability between data spaces is key. An approach to systematically address the interoperability challenges is provided by the new European Interoperability Framework.[45] The framework distinguishes four interoperability levels (technical, semantic, organisational and legal interoperability) that needs to be addressed (see Figure 2).

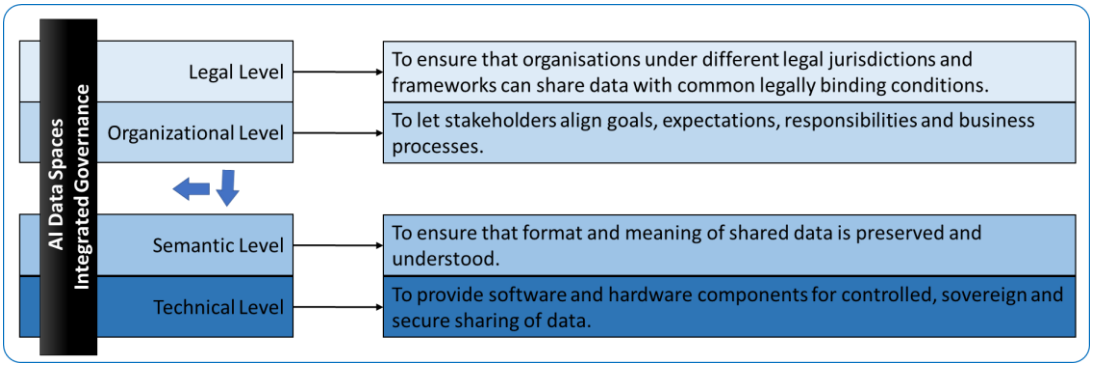


Figure 2. Layered functional model as aligned with the New European Interoperability Framework.

In view of this European ambition on federation of European data spaces, there is a need for adequate governance to realise interoperability within and across data spaces. Therefore, a distinction is made on two development lines:

1. *Intra data space interoperability,* between the (building blocks) within individual data spaces. From that perspective it is to be noted that intra data space interoperability is aimed at providing a reference architecture based on common building blocks and evolution path for developing data space instances in an efficient and aligned manner, providing a rich set of features to support the challenges and requirements for data sharing whilst retaining data sovereignty. It leaves individual data spaces the option for internally deviating from the reference architecture.
2. *Inter data space interoperability,* between multiple data space instances. Interoperability between AI data space instances is key for the federation of AI data spaces to seamlessly interconnect, aligning with the EU data strategy. Inter data space interoperability requires prescriptive guidelines for individual data space instances to ensure interoperability between them. Currently multiple initiatives on inter data space interoperability are emerging. Specifically the work of the Data Sharing Coalition[46] is to be noted. In their 'Data Sharing Canvas' [47], a comparison has been made between various harmonisation options for inter data space interoperability. A motivation is

[44] IDSA. "Use cases are IDS in action". Https://internationaldataspaces.org/make/use-cases-overview/
[45] European Union (2017). "New European Interoperability Framework (EIF) – Promoting seamless services and data flows for European public administrations".
URL: https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf.
[46] The Data Sharing Coalition is an open and growing, international initiative in which a large variety of organisations collaborate to drive cross-sector data sharing at scale.
[47] Data Sharing Coalition (2021). "Data Sharing Canvas - A stepping stone towards cross-domain data sharing at scale". URL: https://datasharingcoalition.eu/app/uploads/2021/04/data-sharing-canvas-30-04-2021.pdf.

provided for preferring the partial harmonisation model by means of a ‘data space proxy’. The role of a proxy is to absorb the complexity of harmonisation for data spaces and its participants as much as possible by implementing all harmonisation requirements. This enables a data provider in one data space to share data with a data consumer in another data space, while limiting impact for both the data provider and the data consumer. Both intra and inter data space interoperability development lines are illustrated in in Appendix A

Various initiatives are developing reference architectures for (data spaces for) controlled data sharing. Their associated technologies are maturing. As such the European reference architectures described in Appendix B are currently emerging that may be considered for implementing data spaces.

2.2.4 Algorithms

The fourth digital technology layer, algorithms, concerns approaches for machine learning and other aspects of artificial intelligence. Algorithms can be described as a series of steps captured in formulas that consist of elements from conditional logic. Such descriptions are meant to automate (and thereby also standardise) a certain process that produces an output based on some input. Algorithms can be described in many languages or forms, but the most common would be mathematical. One of the main areas of interests recently within the field of AI is machine learning. Machine learning is a sub-field within Artificial Intelligence that deals with forms of (semi) autonomous learning based on data.

Machine learning involves the processes and algorithms to obtain correlations from dataset in an automated manner. The field has become a focal point of recent technological and societal artificial intelligence and has thereby a large implication for the future competitiveness of Europe.[48] Important application areas for machine learning are amongst others: image and speech recognition, traffic prediction, self-driving cars, online fraud detection.

There are enormous promises attributed to machine learning, as well as novel risks (for instance around explainability and bias). The economic potential of AI and algorithms is huge but will only be successful when it meets the safety, security and ethical requirements posed by our society.[49] Market prospects of AI enabled systems depend on societal and sectorial adoption and acceptance. Important elements for adoption and acceptance are transparency and explicability of AI systems and their underlying data infrastructures that guarantee trust and sovereignty. Therefore the European Commission took various initiatives;

- They selected a High-Level Expert Group that published the Ethical Guidelines for Trustworthy AI in April 2019.
- In February 2020 they released a White Paper on AI defining a set of features a trustworthy AI system should have.
- They proposed AI regulation, the AI Act, a first-of-a-kind regulation forbidding certain uses of AI algorithms and defining high risk applications where AI algorithms need to be carefully assessed.

[48] https://ellis.eu/

[49] - AI Oversight Lab: Developing trustworthy AI algorithms for public authorities https://nlaic.com/en/use-case/ai-oversight-lab-developing-trustworthy-ai-algorithms-for-public-authorities/

However, there are some challenges for the Netherlands and Europe involved. First, at the level of machine learning, Europe needs an impulse to keep up with the top labs located in North America.[50] Second, despite its strong research on AI and machine learning, Europe has been rather tentative in responding to the industrial and societal challenges around it.[51] The talent retention rate needs to be improved through a stimulating business ecosystem. Besides that there is a too large dependency on non- European countries, since many companies doing top research in this field are situated or controlled elsewhere, outside of the EU. The road for Europe to build trusted AI applications is not trivial; since non- European high-tech giants are currently sitting on the necessary data pools that are enabling for algorithms and machine learning applications. AI applications in Europe are coping with a scaling issue due to a shortage of data access.[52] At the same time, the use of algorithmic systems (especially those of non-European Big Tech company's such as Facebook) raises challenges concerning algorithmic biases not only for the sector in which they operate, but also for society as a whole. Another concern relates to the general view that the Netherlands and Europe are too far behind for the first and even second generation of AI, which means that they should concentrate on the next generations. [53] For example, there are investment gaps in private equity investments in artificial intelligence. Worldwide, about 80% of the investments are in US and Chinese firms, and only 8% in European firms.[54] That makes the Netherlands and Europe dependent on imported AI from outside Europe.

2.2.5 Applications

The fifth digital technology layer, the applications, concern the end-user applications and graphical user interfaces.

Given the high dependence of the previous digital technology layers on non-European countries, it is no surprise that this dependence is extended to the application layer. For more details on this dependence see Chapter 3 in which some domains are described.

However, there are also areas in which the Netherlands and Europe are still strong. The Netherlands and Europe are for instance still strong in equipment manufacturing, in particular complex equipment requiring high precision manufacturing. The market for such products will expand as we move into the digital anything – everywhere era. Examples include e.g. mobility, healthcare, manufacturing equipment and the built environment. As the equipment becomes much more digital, the Netherlands and Europe have the potential to lead the way.

---

[50] https://ellis.eu/ellis-position-paper

[51] European Artificial Intelligence (AI) leadership, the path for an integrated vision, Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies, https://www.europarl.europa.eu/RegData/etudes/STUD/2018/626074/IPOL_STU(2018)626074_EN.pdf

[52]https://www.coe.int/en/web/freedom-expression/algorithms-and-human-rights and https://eu.usatoday.com/story/opinion/2020/07/29/big-tech-abuses-consumers-stop-online-discrimination-column/5525703002/ and New EU AI regulation: Ambitious but disappointingly vague - Tech Monitor and communication-european-strategy-data-19feb2020_en.pdf (europa.eu) and Why Europe's Digital Economy Will Soon Swim Without Data Pools | by Daniel Rebhorn | Towards Data Science

[53] Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry – European Council on Foreign Relations (ecfr.eu)

[54] Organisation for Economic Co-operation and Development: "Private Equity Investment in Artificial Intelligence".

This has lead Germany to focus on edge computing in manufacturing to make factories smarter, for example.

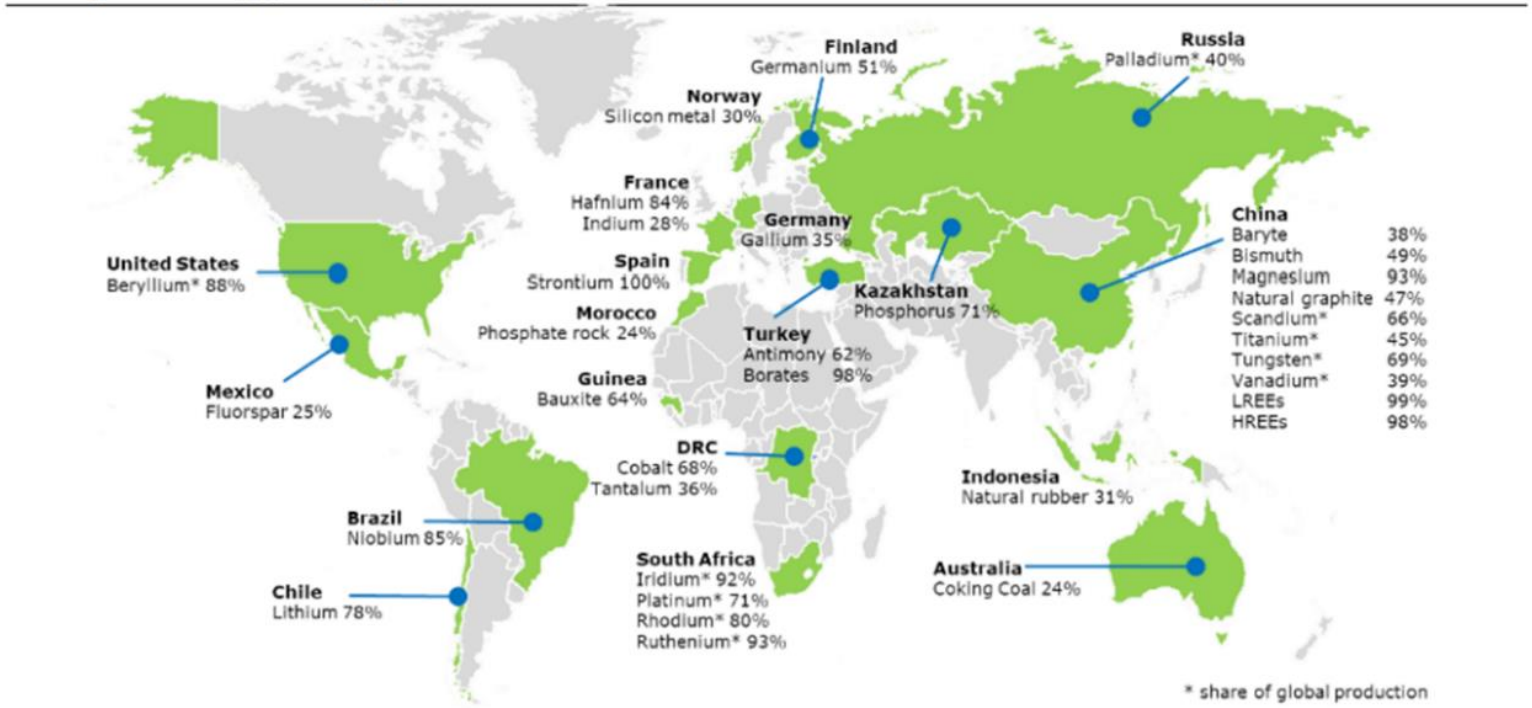
2.3 Influencing factors

Materials and components are the crucial influencing factors of the intermediate and final digital technologies and products.

Manufacturers in the Netherlands and Europe are becoming increasingly dependent on US and Asian imports, mostly in the shape of intermediate or final products in which materials and components are incorporated. These (intermediate) products are part of supply chains that produce electronic components such as microchips and batteries. Rare earth elements are an example of a group of raw materials that are part of strategic decisions, made outside Europe, to control the production of essential modern devices.[55] Other resources such as the high-purity, high-quality process chemicals used in the production process are equally important.[56] Demand is also increasing for new, high-tech raw materials, for example functionalised materials such as quantum dots.[57] In recent decades, the early supply stages of the chain for many of these raw materials and intermediate products have moved to Asia (caused by the fact that China have bought large parts of Africa to mine these raw materials). Box 1 gives an overview of the country of origin of critical raw materials.[58]

[55] https://en.acatech.de/publication/digital-sovereignty
[56] Ibid
[57] Ibid
[58] swd-strategic-dependencies-capacities_en.pdf (europa.eu)

Box 1 Suppliers of critical raw materials



Source: European Commission, Study on the EU's list of Critical Raw Materials (2020)

The intermediate product field can be characterised by complex international supply chains, that are highly dependent on non-EU markets. [59] A good example is the microchip industry. More details on the chip industry are described in section 2.4 about potential disrupting factors. In some cases, this dependency is reciprocal with non-EU parts of the chain relying on products manufactured in the EU (e.g. large parts of the semiconductor supply chain are dependent on ASML).

A stronger focus on circular economy strategies is one of the solutions to reduce Europe's dependence on non-European countries. Circularity means that the raw materials, intermediate products and final products that are already in the hand of the European will retain their value, be it in the shape of intensified use, re-use of components or advanced meta-recycling.

2.4 Potential disrupting factors

We also included some potential disrupting factors to the technology level model, that might change the current digital landscape and could turn the current digital sovereignty status of the Netherlands and Europe. These are smaller, cheaper and more powerful hardware (see section 2.4.1) and new paradigms for cryptography & quantum technology (see section 2.4.2).

2.4.1 Smaller, cheaper and more powerful hardware

The first potential disrupters are the following hardware that become smaller, cheaper, more powerful and thereby more competitive than non-European alternatives: (1) EUV for ICs, (2) batteries, and (3) antennas.

EUV for ICs

The first important hardware, extreme ultraviolet lithography (EUVL or EUV), is the world's most advanced technique to 'draw' the various structures that make up an Integrated circuit (IC).[60] ICs (also called chips) are enabling for digitalisation in general and thereby in all application areas. Chips have enabled increased data storage, real- time data processing at the edge and the manifestation of IoT and AI in value chains worldwide.[61] Other important application areas are the defense and space industry and the automotive sector for instance.

In recent decades, the number of transistors per chip has doubled every two years.[62] The exponential decline in computing power costs will continue in the coming years.[63] There are numerous paths forward to continue performance scaling [64]:

1. The near-term focus will be on development of more specialised architectures and advanced packaging technologies that arrange existing building blocks (see the horizontal axis of Figure 3).
2. In the mid-term, emphasis will likely be on developing Complementary Metal-Oxide Semiconductor (CMOS)-based devices that extend into the third, or

[59] https://en.acatech.de/publication/digital-sovereignty/

[60] https://bits-chips.nl/artikel

[61]https://www.criticalmanufacturing.com/blog/semiconductor-industry-sluggish-digitalization-and-a-way-forward/

[62]https://www.rijksoverheid.nl/documenten/kamerstukken/2021/04/26/toekomstverkenning-digitalisering-2030

[64] https://royalsocietypublishing.org/doi/10.1098/rsta.2019.0061

vertical, dimension and on improving materials and transistors that will enhance performance by creating more efficient underlying logic devices (see the vertical axis of Figure 3). This enhancement of performance will require an increase in raw material demands for pure silicon metal, zirconium, titanium or even hafnium. Current global mining developments suggest that it should be possible to meet this demand.

3. The third axis represents opportunities to develop new computation models such as neuro-inspired or quantum computing, which solve problems that are not well addressed by digital computing.
4. Photonics based computing and spintronics are two other upcoming technologies. Photonic based computing is as the name suggests, a computer system that uses optical light pulses to form the basis of logic gates rather than electrical transistors.[65] Spintronics is and emerging field for the next-generation nanoelectronics devices to reduce their power consumption and to increase their memory and processing capabilities.[66]

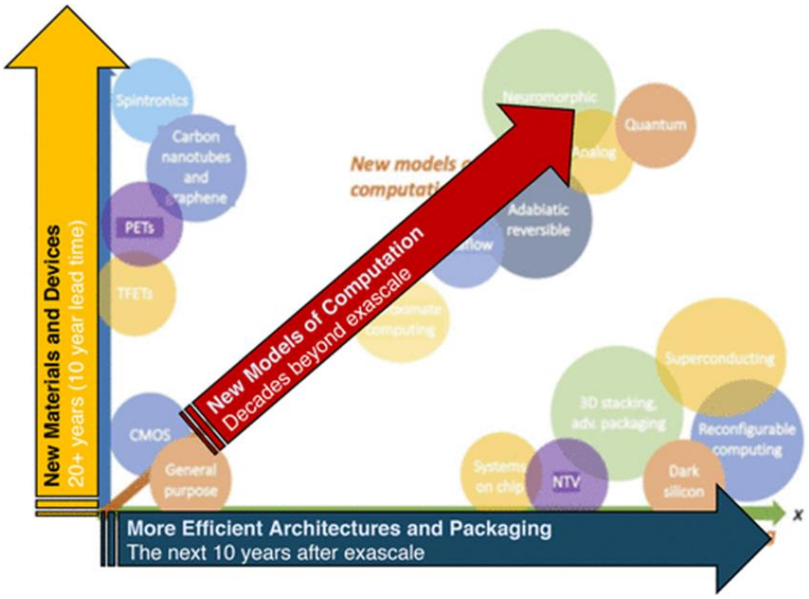


Figure 3. Potential paths to realize continued performance improvements[67]

The shortage of chips (due to more demand than supply) has highlighted one of Europe's vulnerabilities, prompting the European Commission (EC) to set targets to bring the region's share of global chip production to 20% by 2030.[68] The EC also aims to ramp up chip production using the most advanced manufacturing technologies (5nm node and below).[69] Although there is a strong dependence within the chip value chain on the Dutch company ASML, the sole supplier of EUV machines[70] there is also a strong dependence on for instance Taiwanese chip manufacturer TSMC. However, the dependence for the Netherlands and Europe on

[65] https://www.redsharknews.com/photonic-computers-the-future-of-computing-is-analogue
[66] https://www.sciencedirect.com/science/article/pii/S0304885320302353
[67] The future of computing beyond Moore's Law, Volume: 378, Issue: 2166, DOI: (10.1098/rsta.2019.0061) https://royalsocietypublishing.org/doi/10.1098/rsta.2019.0061
[68]https://www.eulerhermes.com/en_global/news-insights/economic-insights/Semiconductors-realpolitik-A-reality-check-for-Europe.html
[69] Ibid
[70]https://www.economist.com/business/2020/02/29/how-asml-became-chipmakings-biggest-monopoly

non-EU countries is stronger than for other parts in the world [71] (such as China, which is less dependent on others) when looking at the following levels in the IC value chain:

1. At the *functional level* on the delivery of processors for AI, data processing and communication such as 5G;
2. At the *design level* on basic design software tools; chip production; and equipment for chip production and testing equipment. At the same time, all these elements are priority areas for obtaining digital sovereignty.[72] We see a comparable picture when we look at the digital capabilities scoreboard that shows that the EU is also behind in the number of producers of AI chips, with 12 firms in the EU, while China has 36 firms and the US 55 firms.[73]

Concerning the High-end microchips using the five nanometre process and beyond (More Moore)[74]: there is no easy way to address the technology dependence that currently exists. The only companies capable of producing these high-end chips are Taiwan's TSMC, South Korea's Samsung and Intel from California. For the current status of the Microchips see Figure 4.[75]

[71] Based on expert input.
[72] Acatech. Digital Sovereignty. Status Quo and Perspectives. https://en.acatech.de/publication/digital-sovereignty/
[73] https://www.oliverwyman.com/our-expertise/insights/2020/sep/european-digital-sovereignty.html
[74] https://en.acatech.de/publication/digital-sovereignty/
[75] Ibid

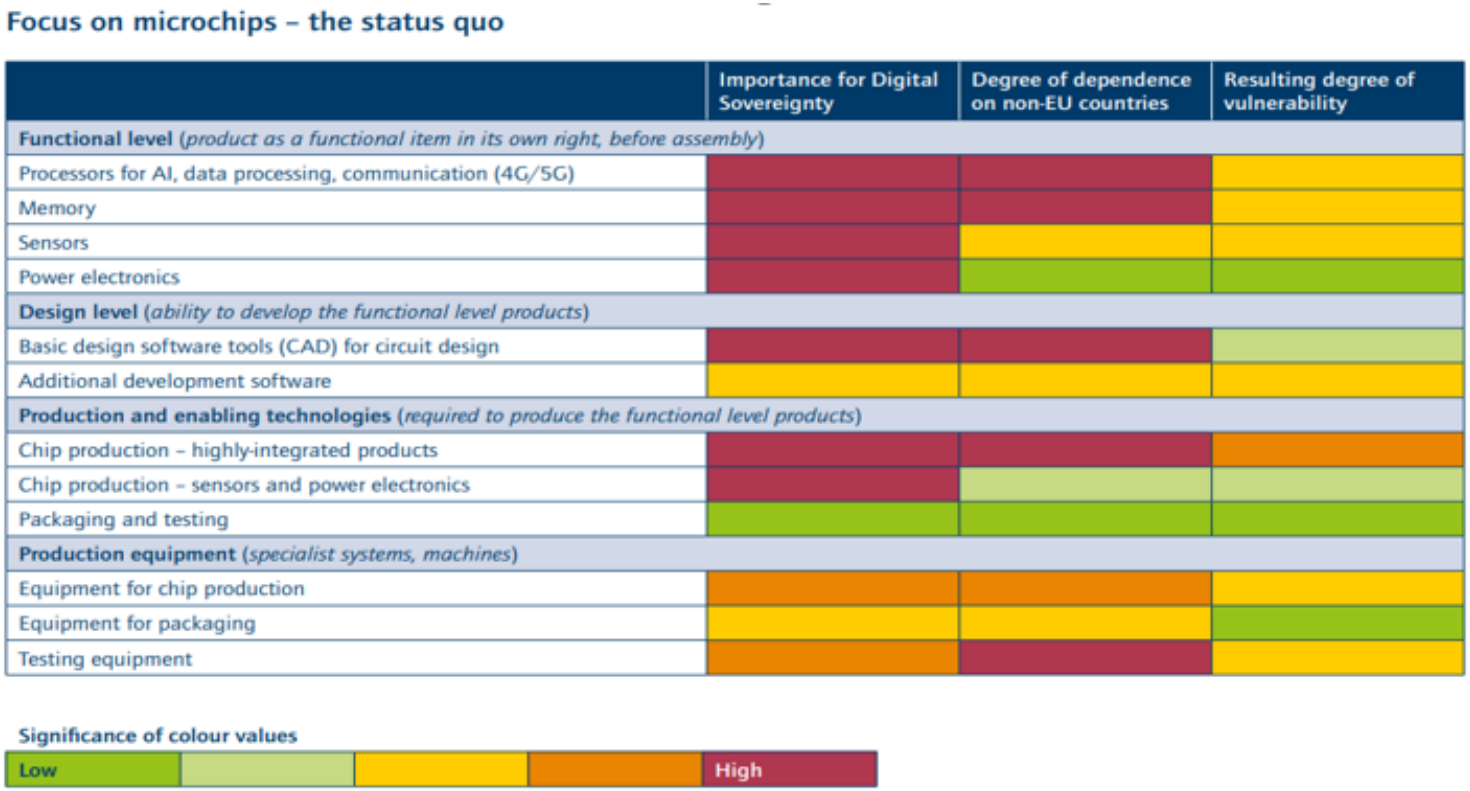


Figure 4. Microchip related priority areas in terms of digital sovereignty[76]

[76] https://en.acatech.de/publication/digital-sovereignty/

However, the EU is unlikely to close the gap on the market leaders in every area, and it would in any case be economically inefficient to do so. Therefore, EU IC manufacturers should be encouraged to identify relevant future IC and production technologies and enter the corresponding markets as soon as possible so that they can build a strong position in them and become a control point. Control points are companies that play an important role in the value chain (e.g. NXP, Infineon).

Batteries

The second important hardware, (rechargeable) batteries, are a strategic part of Europe's clean and digital transition and a key enabling technology.[77] A battery is a source of electric power consisting of one or more electrochemical cells with external connections[78] for powering electrical devices such as laptops, mobile phones, electric cars etc.

Rechargeable battery types include lead-acid, lithium-ion, nickel-metal hydride, and nickel-cadmium batteries.[79] Raw material supply for rechargeable batteries is the front and centre of European ambitions to reduce reliability of non-EU countries for these materials.[80] At the moment, large parts of the Lithium-ion battery (LiB) supply chain are dominated by China and battery mineral prices are experiencing a great deal of volatility, with ripple effects throughout the supply chain. [81] The European Commission wants to change this situation and aims to make Europe a global leader in sustainable battery production and use.[82] That is why the European Commission launched the European Battery Alliance (EBA) in 2018, to build a competitive, sustainable and innovative battery ecosystem in Europe, covering the entire value chain, from raw materials' ethical sourcing and refining, battery cell and pack production, to recycling and re-use.[83] In 2020 EBA had attracted over 500 industrial and innovation actors within 3 years and secured some €100 billion in investments along the entire value chain, thanks to the European Investment Bank.[84]

By 2025, the demand for lithium could triple, partly due to the interest in electric cars. Since there is a limit to the winning of lithium, the metal is on the long term expected to be replaced by light metals such as sodium or potassium [85] with the main benefit that these are much more common, which would lower the production costs of electric batteries.[86] However, also for these alternative materials[87] Europe is also often dependent on non- European countries.

Future progress in batteries heavily rely on the optimization of involved battery components (e.g. Si or Li metal as anode and all solid state batteries) and

[77] https://ec.europa.eu/growth/industry/strategy/industrial-alliances/european-battery-alliance_en
[78] Crompton, T. R. (20 March 2000). Battery Reference Book (third ed.). Newnes. p. Glossary 3. ISBN 978-0-08-049995-6.
[79]https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689337/EPRS_BRI(2021)689337_EN.pdf
[80] https://ec.europa.eu/growth/industry/strategy/industrial-alliances/european-battery-alliance_en
[81]https://hcss.nl/report/batteries-require-battery-minerals-should-europe-ramp-up-its-efforts-to-secure-them/
[82] https://ec.europa.eu/growth/industry/strategy/industrial-alliances/european-battery-alliance_en
[83] https://www.eba250.com/batteries-a-european-success-story/?cn-reloaded=1
[84] Ibid
[85] Grondstoffen elektrische auto: accu | Audi Nederland > The road to zero emission > Modellen > Home > Audi Nederland
[86] Ibid
[87] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0474

lubricants.[88] Attention will focus on material composition and surface coatings of the electrodes as well as the electrolyte used to maximize energy output, while also ensuring safety.[89] Europe also designated battery production as IPCEI (Important Project of Common European Interest) which has led to significant increase in battery cell manufacturing in Europe, although a large part of these factories are still in the hands of non-European companies such as Samsung, LG Chem, CATL, and Tesla.

Antennas

The third important hardware, new antenna technology, has been developed to make long-distance communication possible for a fast form of 5G and its successor, 6G.[90] Antennas, especially the new ones, enable signals at high frequencies (such as 6G) or even longer distances.[91] Think of technology that uses a constellation of electronically-controlled antennas, which electronically steer the radio beams in the right direction.[92]

Antenna technologies are expected to play a pivotal role in telecommunication. With IoT, 5G and 6G communications, the adoption of suitable antenna systems will expedite commercialization of solutions which can support high-speed communications[93] for various domains in the Netherlands and Europe. Dutch firms such as NXP and Ampleon are strong players in this domain on component level.[94]

2.4.2 New paradigms for cryptography & quantum technology

The second potential disrupters are cryptography and quantum technology (quantum computing, quantum (internet) networking and quantum sensing). Cryptography are the secure communications techniques that allow only the sender and intended recipient of a message to view its contents. Data is encrypted using a secret key, and then both the encoded message and secret key are sent to the recipient for decryption.[95] Europe is well positioned in the cryptography domain.[96] An important new development in this domain is post-quantum cryptography. This refers to cryptographic algorithms (usually public-key algorithms) that are thought to be secure against a cryptanalytic attack by a quantum computer.[97]

Quantum technology is a key technology that enables new products and services. Quantum computers, quantum simulators, quantum networks and quantum sensors will soon be able to do things that their 'traditional' predecessors cannot.[98] The Netherlands has a strong position in quantum (internet) networks and quantum key

[88] https://journals.sagepub.com/doi/full/10.1177/16878140211021730
[89] Ibid
[90]https://www.tue.nl/en/our-university/departments/electrical-engineering/department/news/news-overview/new-antenna-technology-for-extremely-fast-5g-and-6g-successfully-tested-on-tue-campus/
[91] https://www.tue.nl/en/our-university/departments/electrical-engineering/department/news/news-overview/new-antenna-technology-for-extremely-fast-5g-and-6g-successfully-tested-on-tue-campus/
[92] Ibid
[93]https://www.businesswire.com/news/home/20200218005900/en/Antenna-Technology-2019-Expected-to-have-a-Major-Impact-on-High-Speed-Data-Transfer-Next-Generation-Wireless-Communication---ResearchAndMarkets.com
[94] Based on expert input.
[95] https://www.kaspersky.com/resource-center/definitions/what-is-cryptography
[96] https://en.acatech.de/publication/digital-sovereignty
[97] https://www.cbinsights.com/research/post-quantum-cryptography/
[98]https://www.tno.nl/en/focus-areas/industry/roadmaps/semiconductor-equipment/quantum-technology/

distribution.[99] Quantum technology is still in the early stages of development and its practical applications today are still limited. But by 2030, it is likely according to the experts that quantum technology will be a vital technology (e.g. quantum computing) with projected benefit across a range of application areas including communication, industry, and AI, among others.[100] The first generation quantum networks will be available within some years from now.[101]

Germany and France are already pushing forward in this sector.[102] But also Belgium, Germany, Italy, Luxembourg, Malta, the Netherlands, and Spain recently signed a declaration agreeing to explore together, over the next 12 months, how to develop and deploy a European Quantum Communication Infrastructure (EuroQCI) within the next ten years.[103,104]This infrastructure would enable information and data to be transmitted and stored ultra-securely, and link communication assets all over the EU.[105] It would integrate quantum technologies and systems into conventional communication infrastructures, and consist of two important elements[106]: 1. an earth-based component making use of existing fibre communication networks linking strategic sites at national and cross-border level, and 2. a space-based component to cover long distances across the EU and other continents.

The analysis of all technology layers indicates that the Netherlands and Europe are highly dependent on non-European countries. This means that the Netherlands and Europe are less digital sovereign compared to the US and China. This difference in digital sovereignty is partly caused by the different models that the EU, US and China apply. Box 2 explains the differences between these models.

[99] Based on expert input.
[100] https://dgap.org/sites/default/files/article_pdfs/210422_report-2021-6-en-tech.pdf
[101] Based on expert input.
[102] https://dgap.org/sites/default/files/article_pdfs/210422_report-2021-6-en-tech.pdf
[103]https://digital-strategy.ec.europa.eu/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network
[104] European Quantum Communication Infrastructure (EuroQCI) | Shaping Europe's digital future (europa.eu)
[105] Ibid
[106] Ibid

Box 2: Different models worldwide influencing the digital sovereignty of the Netherlands and Europe [107]:

*The **European model**[108]: "is value- and human rights-based and has a focus on ethics and privacy. The GDPR has enshrined into EU law a universalistic approach to the protection of privacy, extending protection of its citizens in other jurisdictions and enlarging the right of being forgotten. GDPR covers all data processing activities to anticipate and minimise risk. Also, in recent years the EU competition approach has been more proactive including anti-trust initiatives against dominant firms, based on Article 102 of the EU Treaty".*

*The **US model**[109]: "is based on the American tradition and focus more toward liberty and is a mix of a technology and commerce driven approach. With respect to privacy the dominant view is to treat it as tort, where the victim must prove the harm, which is in line with the Silicon Valley attitude to disrupt and move fast before regulation will intervene. In this respect the approach is commercial and there is convergence of views between Silicon Valley and Washington. One characteristic of the US model is the lack of a unified federal framework for data protection and cyber security and the presence of several state laws and other sources of regulation or self-regulation and standardisation. It is remarkable that, as a result of Europe introducing GDPR and other measures, there is mounting pressure in the US for a federal standardisation on data privacy and cybersecurity".*

*The **Chinese model**[110]: "promotes its own tech giants (such as Baidu, Tencent and Alibaba) which work under close governmental control. These firms are less complacent, more vigorous, more eager for competition, and less constrained than their US or European counterparts. An important advantage of China is also its implementation capacity. China has the advantage of both the national skillset and the numbers of scientists it can deploy. Data protection in China is not up to European standards in terms of values and rights. China's cybersecurity market is, to all intents and purposes, driven by the government. It is dominated by large monopolies with strong links to national security with probably negative effects on the provision of cybersecurity. Moreover, its Internet economy generates more data than any other. Lastly, unhindered by data protection regulation or noticeable public demand for privacy, data is gathered from many other sources, including closed circuit television."*

2.5 Boundary condition factors

Next to the potential disrupting factors, boundary condition factors such as policy measures (see section 2.5.1) and business models (see section 2.5.2) can turn the current digital sovereignty status of the Netherlands and Europe (e.g. by scaling and stimulating technological solutions that are based on digital sovereignty principles such as decentralised architectures).

2.5.1 Policy measures

In this section we elaborate in more detail on the first boundary condition factor; the policy measures applied by policy makers such as the European Commission and the Member states to increase their digital sovereignty. We distinguish four governmental roles and instruments[111] that are executed or can be executed by policy makers to stimulate digital sovereignty (see Figure 5). Each of the instruments are discussed below.

[107] https://www.eitdigital.eu/fileadmin/files/2020/publications/data-sovereignty/EIT-Digital-Data-Sovereignty-Summary-Report.pdf
[108] Ibid
[109] Ibid
[110] Ibid
[111] https://www.kimnet.nl/binaries/kimnet/documenten/notities/2018/09/03/nieuwe-tijden-nieuwe-overheidsinstrumenten/Nieuwe+tijden+nieuwe+overheidsinstrumenten.pdf

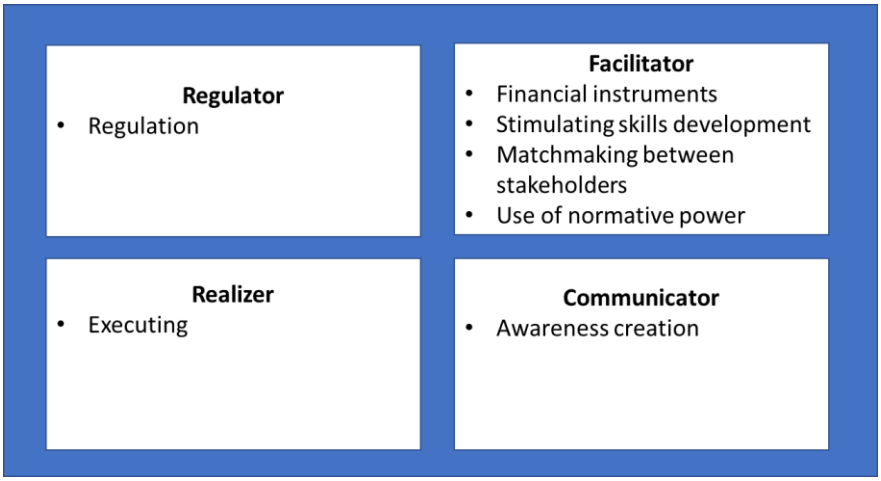


Figure 5. Roles of the government and related policy instruments[112]

Regulator

In its role as regulator, the government initiates a desired behaviour by prescribing or prohibiting certain activities by means of rule- and norm-setting.[113] Being a regulator is one of the EU's greatest strengths to set global technical standards in a number of fields ("the Brussels effect"). Accordingly, the strive for "tech sovereignty" has a clear connection with the EC's "coordinated European approach" – its regulatory stance and efforts towards completing the digital single market. Digital sovereignty underpinned by a comprehensive regulatory program is expected to provide European developers and manufacturers with a much-needed competitive edge, and consumers and users with products adhering to high ethical, democratic, and human-rights standards (as opposed to such originating from the US or China).

Regulation

Regulation is seen as a vital instrument of the EU's strategy for catching up with the US and China in the global digital race, providing space for Europe to make its own innovation and governance choices. The EU wants to deliver on the promise of human-centered and risk-based new tech regulation, together with a comprehensive regulatory packaging including the[114]; European Digital Strategy, the European Data Strategy, the Digital Services Act, the Digital Markets Act, as well as the White Paper on Artificial Intelligence and the EU's latest AI regulation package. The EU has however a harder time in setting global rules and red lines.[115] For an extensive analysis of the European regulation relevant for Digital sovereignty see appendix C and D

Facilitator

In the role of facilitator, the government creates conditions that allow third parties to encourage desired behaviour.[116] The European Commission and the Member

[112] Based on: https://www.kimnet.nl/binaries/kimnet/documenten/notities/2018/09/03/nieuwe-tijden-nieuwe-overheidsinstrumenten/Nieuwe+tijden+nieuwe+overheidsinstrumenten.pdf
[113]https://www.kimnet.nl/binaries/kimnet/documenten/notities/2018/09/03/nieuwe-tijden-nieuwe-overheidsinstrumenten/Nieuwe+tijden+nieuwe+overheidsinstrumenten.pdf
[114] https://carnegieeurope.eu/2021/08/12/eu-s-rise-as-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty-pub-85134
[115] Ibid
[116]https://www.kimnet.nl/binaries/kimnet/documenten/notities/2018/09/03/nieuwe-tijden-nieuwe-overheidsinstrumenten/Nieuwe+tijden+nieuwe+overheidsinstrumenten.pdf

states are applying facilitation instruments such as financial instruments, stimulation of skills development, matchmaking and the use of normative power.

Financial instruments

The European policy makers provides various financial instruments[117] that contribute direct or indirect to digital sovereignty. Examples are described in Box 3.

Box 3 Examples of financial instruments that contribute to digital sovereignty

- The **Digital Europe Programme**[118] is the programme of the European Commission designed to fill the gap between research and deployment of digital technologies with the public funding of €7.6 billion between 2021 and 2027. Specifically, the program consists of components targeting Artificial Intelligence, the European Digital Innovation, Cybersecurity and High Performance Computing.
- **Horizon Europe**[119] provides specifically for 'Digital, industry and space': 35% of €95.5 billion of public funding between 2021 and 2027, targeting the research on enabling technologies complementing the Digital Europe Programme such as 5G, high performance computing, cloud computing and AI.
- Within the **Connecting Europe Facility** (CEF), there is Digital strand[120]. With the available funding of €2.07 billion between 2021 and 2027, CEF – Digital provides support and investments in digital connectivity infrastructures of common interest, trans-European networks and infrastructures in the transport, telecommunications and energy sectors. This program is a predecessor of the first generation of the CEF Telecom strand, that targeted connectivity in local communities and broadband networks and deployed digital service infrastructures.
- Together with the European Investment Fund, the European Commission launched six Venture Capital funds[121] under the **InnovFin Artificial Intelligence and Blockchain** pilot[122] in October 2020. These funds provide a total of €700 mln for digital start-ups and SMEs in early- and growth stages to stimulate scalable activities in Artificial Intelligence and Blockchain technologies.
- In response to the COVID-29 pandemic, the **InvestEU**[123] program was set up. Within this program, approximately €3 billion is made available in public funding to improve connectivity, widespread use of digital technologies and infrastructures and skills. This program is part of larger effort combining both public and private funding.
- Other programs, such as **EU4Health**[124], **Recovery and Resilience Facility**[125], are also available for companies. Stimulation of the digital transformation is part of it.

Stimulating skills development

European policy makers also facilitate skills development. This is especially important since the EU is lagging behind with digital talent.[126] China and India have produced fast-growing numbers of STEM (science, technology, engineering, and mathematics) graduates. The two countries are expected to account for more than 60% of the STEM graduates in major economies by 2030, compared to only 8% for Europe and 4% for the United States.[127] Examples of skills development initiatives are described in Box 4.

[117] The list is not exhaustive, but some illustrative examples are provided.
[118] Digital Programme | Shaping Europe's digital future (europa.eu)
[119] https://digital-strategy.ec.europa.eu/en/activities/funding-digital
[120] Connecting Europe Facility (europa.eu)
[121] Six Artificial Intelligence and Blockchain Technology funds (europa.eu)
[122] EFSI Equity instrument (eif.org)
[123] InvestEU | InvestEU (europa.eu)
[124] EU4Health 2021-2027 – a vision for a healthier European Union | Public Health (europa.eu)
[125] Recovery and Resilience Facility | European Commission (europa.eu)
[126] Organisation for economic co-operation and development: Skills Outlook, https://www.oecd.org/education/oecd-skills-outlook-e11c1c2d-en.htm
[127] https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2020/october/European%20Digital%20Sovereignty.pdf

Box 4 Example of digital skills development initiatives in Europe:

- **The European Commission** is determined to tackle the digital skills gap and promote projects and strategies to improve the level of digital skills of the European.[128]
- **The Digital Education Action Plan** (2021-2027) is a renewed European policy initiative to support the sustainable and effective adaptation of the education and training systems of EU Member States to the digital age. [129]
- To support both priority areas, the Commission will establish a **Digital Education Hub**[130] to cooperate and exchange in digital education at the EU level.
- The **DIGITAL Europe programme will fund the design and delivery of specialised programmes and traineeships** for future experts in key capacity areas like data and AI, cybersecurity, quantum and HPC.
- The European **Digital Skills and Jobs Platform**[131] is a new initiative launched under the Connecting Europe Facility Programme. It offers information and resources on digital skills, as well as training and funding opportunities.
- **All Digital**[132] supports Europeans that have an insufficient level of digital skills.
- The ·**MyDigiSkills**·system has been created under a Creative Commons Licence by ALL DIGITAL from the DigCompSAT project of the Joint Research Council of the European Commission.[133]
- Jointly with the Digital Europe Programme and the Recovery and Resilience Facility, the **Digital skills and job platform** will contribute to the objectives of Europe's Digital Decade, namely that 80% of Europeans will have at least basic digital skills and that there will be 20 million employed digital technology experts by 2030. It will also contribute to a shared engagement model for skills development in Europe.[134]
- **Train-the-trainer programs** via for instance Digital Innovation Hubs and alike.
- There are also **national programs**, such as the national AI course, inspired by the Finish example (see[135]).
- The **Skills recognition program of the BDVE** addresses the needs of data scientists, industry, and academia while taking into consideration educational trends in Europe.[136]
- There has been a specific focus in the recent decade on **promoting women in STEM sciences**[137], and for women in data science and AI specifically as well[138].

Matchmaking between stakeholders

The European policy makers also fulfill a matchmaking role by organising various conferences and events such as:

- The Data and AI event in December 2021.[139]
- Former Big data value forums around centres of excellence on Big data in Europe.[140]
- DigitalSME organizes and facilitates SME interaction and innovation in Europe[141]

[128] https://digital-strategy.ec.europa.eu/en/policies/digital-skills-and-jobs
[129] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en
[130]https://education.ec.europa.eu/focus-topics/digital-education/digital-education-action-plan/digital-education-hub
[131] https://digital-skills-jobs.europa.eu/en/about/digital-skills-and-jobs-platform
[132] https://all-digital.org/about-us/
[133] https://mydigiskills.eu/
[134]https://www.pubaffairsbruxelles.eu/commission-launches-digital-skills-and-jobs-platform-to-accelerate-digital-upskilling-in-europe-eu-commission-press/
[135] https://www.elementsofai.com/
[136] https://www.big-data-value.eu/skills/skills-recognition-program/
[137] Women in science and engineering - Products Eurostat News - Eurostat (europa.eu)
[138] Women in AI (#WAI)
[139] https://european-big-data-value-forum.eu/
[140] https://www.big-data-network.eu/
[141] European DIGITAL SME Alliance

Use of normative power

As a facilitator, the European policy makers often uses their normative power (the ability to cause effects by means of spreading European values and norms)[142] in external partnerships to obtain desired positions or to lay the foundation for those. There are a number of mechanisms used in that regard – persuasion, discourse shaping, leading by example or explicitly invoking/ propagating particular norms. With regard to digital sovereignty, the EC has been making use of discourse shaping (with, for instance, the rhetoric of "AI made in Europe", "human-centric AI", "the digital decade", etc.), while when it comes to other aspects of its digital agenda, leading by example and endorsing certain norms is more frequently opted for. The latter is the case with the GDPR and the draft AI act, which are intended among others to spread a particular normative message.

Realizer

As a realizer, the government itself actively ensures the creation of a particular good or service.[143] European policy makers are doing this via public procurement.

Public procurement

Every year, more than 250,000 public authorities in the EU spend about 14% of GDP on the purchase of services, works and supplies.[144] Public procurement refers to the process by which public authorities, such as government departments or local authorities, purchase work, goods or services from companies. To create a level playing field for all businesses across Europe, EU law sets out minimum harmonised public procurement rules. [145] In many sectors such as energy, transport, waste management, social protection and the provision of health or education services, public authorities are the buyers.[146] The public sector can use procurement to boost jobs, growth and investment, and to create an economy that is more innovative, resource and energy efficient, and socially-inclusive.[147] This means that this instrument could also be applied for the digital domain as long as it meets the procurement rules.

Communicator

As a communicator, the government has an informative role focussed on awareness creation.[148]

Policy makers often communicates about the importance of digital sovereignty of Europe. Examples are of such awareness creation are:

- Through communication and information campaigns.
- The various communications from the European Commission such as the document on Shaping Europe's digital future.[149]
- Various speeches that are also published. [150]

---

[142] Forsberg, Tuomas. "Normative power Europe, once again: a conceptual analysis of an ideal type." *JCMS: Journal of Common Market Studies* 49.6 (2011): 1183-1204.

[143]https://www.kimnet.nl/binaries/kimnet/documenten/notities/2018/09/03/nieuwe-tijden-nieuwe-overheidsinstrumenten/Nieuwe+tijden+nieuwe+overheidsinstrumenten.pdf

[144] https://ec.europa.eu/info/policies/public-procurement_en

[145] Ibid

[146] https://ec.europa.eu/growth/single-market/public-procurement_en

[147] Ibid

[148]https://www.kimnet.nl/binaries/kimnet/documenten/notities/2018/09/03/nieuwe-tijden-nieuwe-overheidsinstrumenten/Nieuwe+tijden+nieuwe+overheidsinstrumenten.pdf

[149] communication-shaping-europes-digital-future-feb2020_en_3.pdf (europa.eu)

[150] Such as State of the Union 2020 | European Commission (europa.eu)

European policy makers in Europe often communicate about the following topics related to digital sovereignty: 1. Emerging technologies, 2. Digital Infrastructures, 3. Data governance, 4. Cybersecurity and 5. Constraining platform power.[151] Figure 6 outlines the frequency with which each policy area was cited as being of importance in the period 2020-2021.

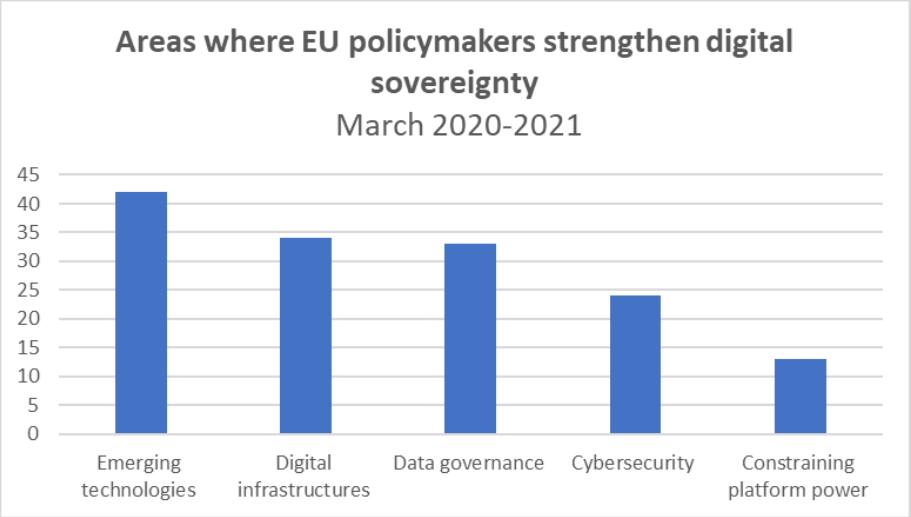


Figure 6. Areas where policy makers strengthen digital sovereignty[152, 153]

2.5.2 *Business models*

In this section we elaborate on the second boundary condition; the business models. We first describe the dominant business model trends after which we discuss how they contribute to digital sovereignty.

An important business model trend is the pursuit of *servitization*, that influence contemporary business models in a domain such as manufacturing. With this business model manufacturers sell for instance no longer only their hardware, but a service built on top of the hardware (while the hardware remains the property of the manufacturer). The data that a manufacturer collects from the hardware that is leased by the customers ensures that manufacturers can improve their hardware and reuse returned hardware or recycle it as efficiently as possible. The advantage is that this contributes to sustainability. At the same time, this data can also warn customers about malfunctions so that early intervention can be taken (e.g. predictive maintenance). Another dominant trend are the *platform-based* business models. We see these business models in domains such as travelling and accommodation provisioning, mobility exchange and social media. In such business models, platform providers facilitate direct supplier-to-customer interactions and exchange of goods and services. These platforms aim to create value for the user by adopting an explicit service-based perspective for its offerings through virtualization or cloudification of the proposed offerings.

[151] https://policyreview.info/pdf/policyreview-2021-3-1575.pdf
[152] Policy review 2021: https://policyreview.info/pdf/policyreview-2021-3-1575.pdf
[153] Based on Google's site search function to collect web pages from the European Commission's, Council's, and Parliament's official websites, between 10 March 2020 and 10 March 2021, that explicitly mentioned the term "digital sovereignty".

However, there is also a downside to these business models, since they increase the dependency (e.g. of the platform users (suppliers and customers) to the platform). This dependency becomes even more apparent when such services are integral to the business logic of the user. As platform users for instance consequently build practices based on such platform system support, such organizations become strongly dependent on such systems, creating *vendor lock-in* and making it difficult to move to another platform. In addition to these dependencies, it also becomes quite difficult for platform users to control how such services are configured. Accordingly, end-users lose their sovereignty in terms of shaping their digital landscape.

Business modelling can help to create clarity on how product or service-based solutions create value for both the platform and users involved. Various European initiatives include digital sovereignty as design principle in their business model, like they did with environmental and social sustainability. They do this for instance for a federated cloud alternative (e.g. Gaia-X[154] or IDSA).[155, 156] Such decentralised solutions require a *collaborative business modelling approach*. There are several examples (e.g. JoinData, SCSN and sqyppi IoT) of collaborative, digitally enabled services that generate significant value for stakeholders and the ecosystem involved. However, how such initiatives should be governed digitally, is still under-investigated. To support the design of business models, several practitioners have focused on the development of business model design tools such as the popular Business Model Canvas[157], but also new types of tools such as the Platform business model canvas. For more details on these tools see Appendix E, as well as the various business roles see Appendix F.

[154] https://www.isst.fraunhofer.de/en/gaia-x/Gaia-X_Fraunhofer-ist-Key-Player.html
[155] https://internationaldataspaces.org/
[156] a European standard for data sharing that enables data sovereignty that brings a “connect-once -reach the entire value chain scenario” to companies
[157] Presented in Osterwalder, Alexander, and Yves Pigneur. *Business model generation: a handbook for visionaries, game changers, and challengers*. Vol. 1. John Wiley & Sons, 2010.

3. Promising innovation areas

The digital technology layers discussed in the previous sections are – by nature – generic. They can leverage developments in various application areas (verticals). Secondly, developments in application areas can constitute a market pull for new digital technologies.

This raises questions on the role of digital sovereignty in promising innovation areas[158] in several verticals such as; How can these verticals become more digital sovereign and operate according to European norms and values? What are the challenges in this context? And how can they constitute a potential market for sovereign digital technologies? We selected six domains to discuss the promising innovation areas and answers related to these questions (see Figure 7). These six domains were selected because:

- Disruptions of digital sovereignty can have high societal costs;
- They have the potential to gain economic or societal improvement when digital sovereignty will be improved; and/or
- Digitalisation is a key enabler in the respective domain.

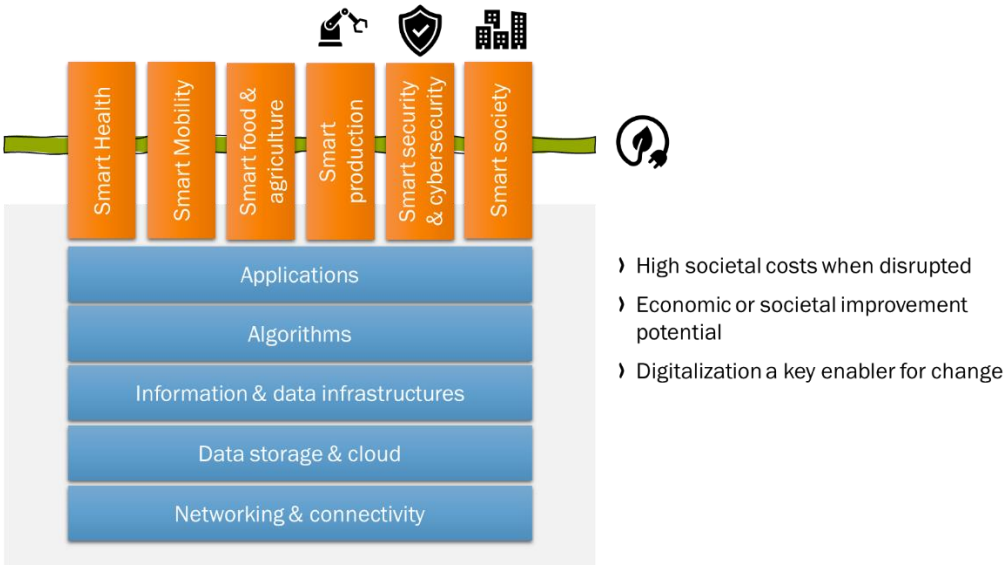


Figure 7. Technology layers and innovation areas

3.1 Smart Health

The Netherlands and Europe face a number of challenges when it comes to providing healthcare. A recent analysis made by the European Commission states the main three[159]:

1. An ageing population and chronic diseases putting pressure on health budgets;
2. Unequal quality and access to healthcare services and;
3. A shortage of health professionals.

[158] These innovation areas build on the TNO study about “Kansrijke innovatie opgaven voor Nederland”: https://publications.tno.nl/publication/34623505/7RjMww/bakker-2017-portfolioanalyse.pdf
[159] eHealth_infographic_20180424 (europa.eu)

All of these issues have been put under a magnifying glass during the Covid pandemic. Digitalisation provides a solution for these challenges and is seen as a way to improve the quality and increase efficiency in healthcare. The pandemic showed an increase in the demand, development and uptake of digital technologies in healthcare.[160] Think of the need for cross-border data transfers, data sharing on outbreaks, the collective development of a framework around privacy-friendly Covid-tracing apps, and finding ways to share and make interoperable apps[161], to name a few.

Promising innovation areas
To further mitigate the three aforementioned health care challenges the following promising innovation areas (enabled by digital technologies) are important[162]:

- Prevention and management of chronic diseases: promoting healthy behavior and health literacy, personal coaching systems based on data from the individual and environment;
- Personalised care: development of individual-oriented diagnostics, treatment methods and medicines;
- New healthcare concepts and models; based on e-health and mobile health for a sustainable healthcare system.

The first promising innovation area contributes to the first challenge by providing preventive solutions to avoid a further increase of chronic diseases of elderly. The second and third areas serve the second and third challenges by providing tools for better personal diagnostic services and to compensate for the lack of healthcare professionals.

Benefits, challenges in the context of digital sovereignty
Digitalisation of healthcare has a strong connection with sovereignty benefits and challenges. Examples of benefits of digitalisation in and of healthcare are widespread and indeed deal with either using digital means and tools to push forward medical sciences[163], data and digital tools to improve medical procedures and standards.[164] Or using digital tools to better help patients and citizens to become autonomous by keeping track of their own data while at the same time allowing for large-scale medical analyses through multi-sided digital platforms[165], for example.

Some challenges in the digitalisation of healthcare, that have a strong connection with sovereignty challenges, are, among others, the national and historically widely varying nature of healthcare systems and levels of digitalisation, often accompanied with a certain level of protectionism when it comes to health data. Moreover, many current systems for health data in the cloud are currently already stored on non-EU clouds [166], making the achievement of full control over health data impossible. Other challenges concern the merger of *lifestylization* and *platformization* of healthcare

[160] The rise of digital health technologies during the pandemic (europa.eu)
[161] Coronavirus: EU interoperability gateway (europa.eu)
[162] Bakker et al. Kansrijke Innovatie opgaven voor Nederland, (2017) TNO report https://publications.tno.nl/publication/34623505/7RjMww/bakker-2017-portfolioanalyse.pdf
[163] Predicting gene expression with AI | DeepMind
[164] European Health Data Space | Public Health (europa.eu)
[165] My Health My Data
[166] See France's health data hub running on Microsoft: Page d'accueil | Health Data Hub (health-data-hub.fr)

that has been mainly pushed by large private ICT horizontals that operate in a context in which healthcare is unaffordable and public alternatives are pretty much non-existent.[167] The risk of this merger are the hyperscaler based business models behind those platforms, next to more generic risks of the loss of privacy and increased security risks.[168] Via data cooperatives and leverages of the current European health data, some form of market power can be exercised[169], and thereby some minimal safeguards on issues such as privacy and security. Yet, the challenging task is to standardize, if we aim to let ICT be supportive for health procedures. Next to that massive investments and efforts are needed to bridge the digital literacy and skills gap in different layers of the healthcare systems.[170]

3.2 Smart Mobility

In the mobility domain, we see that technological innovations such as cooperative intelligent transport systems (C-ITS) and connected and automated driving (CAD) are increasingly shifting the mobility landscape, establishing data-driven (inter)dependencies between mobility and market stakeholders and posing challenges in terms of how such innovations can be deployed throughout Europe.

Promising innovation areas
Such innovations are related to promising innovation areas (enabled by digital technologies) such as[171]:

- Advanced systems of traffic management and logistics in passenger and freight transport (multimodal; sensors, data, IoT);
- Cooperative and autonomous driving based on a combination of smart infrastructure, sensors, data, self-driving cars and laws and regulations.

Benefits, challenges in the context of digital sovereignty
Based on a European project called DIRIZON the innovation areas and digital transformation in the mobility domain will be further illustrated as well as their benefits and challenges related to digital sovereignty. With regards to connected and automated driving, the DIRIZON project[172] has focused on establishing a data-exchange platform driven by national road authorities (NRAs) to support CAD. A benefit is that such a data-exchange platform would facilitate the deployment of 'CAD-fleet-as-a-service' (public and private services in the context of connected automated driving), contributing towards improved and more efficient mobility. Establishing such a platform and scaling the platform in Europe however leads to challenges and poses major questions in terms of orchestration, interoperability and (digital) governance.

---

[167] Sharon, T. (2018). When digital health meets digital capitalism, how many common goods are at stake?. *Big Data & Society*, *5*(2), 2053951718819032.
[168] See Millar SA et al. WannaCry: Are Your Security Tools Up to Date? The National Law Review 2017, https://www.natlawreview.com/article/wannacry-are-your-securitytools-to-date
[169] See Calzada, I. Data Co-Operatives through Data Sovereignty. *Smart Cities* **2021**, *4*, 1158-1172. https://doi.org/10.3390/smartcities4030062
[170] Pastorino, R., De Vito, C., Migliara, G., Glocker, K., Binenbaum, I., Ricciardi, W., & Boccia, S. (2019). Benefits and challenges of Big Data in healthcare: an overview of the European initiatives. *European journal of public health*, *29*(Supplement_3), 23-27.
[171] Bakker et al. Kansrijke Innovatie opgaven voor Nederland, (2017) TNO report https://publications.tno.nl/publication/34623505/7RjMww/bakker-2017-portfolioanalyse.pdf
[172] https://www.dirizon-cedr.com/

In DIRIZON, three scenarios regarding the deployment of this data-driven platform are drafted, which can be summarised as *publicly orchestrated (centralised), privately orchestrated (decentralised)* and a *hybrid orchestration (federated)*:
In the *first scenario*, the EU collectively (involving the National Road Authority's) focuses on the development of a data-exchange platform to support the deployment of CAD in Europe. Whilst this approach helps in fostering the standardization of how the data-exchange platform is configured (reducing the likelihood that digital dependencies are created), it requires all National Road Authority's (NRAs) to be involved for the decision making (an 'agree' first approach before any solutions are constructed). This significantly lengthens the timing for which such solutions can be rolled out on the market.

Alternatively, for the *second scenario*, the role of platform development can be given to OEMs. Whilst this accelerates the pace for which solutions can be presented to the market, it does create dependencies on large-scale private companies and moreover largely is driven by market demand. As a consequence, such solutions tend to be catered to urban areas, whereas wide-scale deployment of the solution in Europe depends on whether other markets can be targeted here, or whether the solutions in different countries can be made interoperable.

A *third scenario*, the hybrid variant, builds upon the beneficial aspects of public and private orchestration by federating the development of platform-based solutions, allowing such solutions to be developed locally (to accelerate the time-to-market of CAD solutions), but to ensure that such a platform is interoperable such that other parties or countries at a later stage can connect their services to the platform (to stimulate the wide-scale deployment).

Each of the scenarios posed different benefits and challenges in the context of digital sovereignty.

3.3 Smart Food & Agriculture

A growing world population and higher incomes are leading to strong global growth in the demand for food. At the same time, the available agricultural land is decreasing due to urbanization, industrialization and erosion.[173] To provide solutions for these challenges the food and agricultural domain is increasingly recognising the value of digitalisation to improve the efficiency of current farming practices and provide a more sustainable way of operations.

Promising innovation areas
Digitisation of food and agriculture builds on the following promising innovation areas such as[174]:

- Intensive and sustainable production systems for food and biomaterials through precision agriculture (NL and worldwide). A range of technologies are used to enable precision farming such as GPS, sensor technology, ICT and robotics;
- Improving agricultural production by integrating plant distribution and crop management – linking data from molecular breeding and production systems.

[173]Bakker et al. Kansrijke Innovatie opgaven voor Nederland, (2017) TNO report https://publications.tno.nl/publication/34623505/7RjMww/bakker-2017-portfolioanalyse.pdf
[174] Ibid

These innovation areas are stimulated by policy makers in the following way; There is a significant push by governments and policy makers to reduce the environmental pollution that result through farming practices. Such environmental pollution is the result from overuse of pesticides and fertilization, whereas farmers have limited insights on how use of resources (e.g. water or soil) can be further improved. As a consequence, the aforementioned innovation areas are increasingly applied by dedicated service providers of smart farming solutions aimed at increasing the transparency of farming practices in terms of pesticides, water and fertilization used, whilst additionally providing farming advice on how to improve the overall quantity and quality. Whilst this helps farmers in improving their operations, it creates dependencies for farmers on data-driven solutions for their operations and to remain efficient and sustainable.

Benefits, challenges in the context of digital sovereignty
Digital sovereignty plays an important role in the food and agricultural domain. Especially in relation to business models. Table 1 displays 7 business model archetypes found in the agricultural domain.[175] Many of these business models rely on data-driven technologies, and thus rely on data crossing organizational borders and digital technologies entering the farm's premises (e.g. data-driven farm optimization, transparent farming practices). In light of the sovereignty of farmers, commercial implementations, contain benefits such as the undeniable value creation for the farmer and other value chain participants, but it may also incur challenges and downsides. Foremost, commercial implementations represent yet-another dependency of the farmer on another business. Such business may change its service conditions unilaterally or, might be taken over by powerful conglomerates (e.g. BASF/Monsanto, John Deere, Google, Microsoft).

[175] https://ploutos-h2020.eu/

Table 1. Business model archetypes[176]

Maximize material and energy efficiency	Create value from waste	Deliver functionality rather than ownership	Adopt a stewardship role	Re-purpose for society	Shorten the value chain*	Support financial stability*
Products or services that use fewer resources, generate less waste and emissions and create less pollution than products that deliver a similar functionality	Turning existing waste streams into useful and valuable input to other production	Provide services that satisfy user needs without users having to own physical products	Manufacture products and services intended to genuinely and pro-actively engage with stakeholders to ensure their long-term health and well-being. Better engaging the consumer with the full story of production and the supply chain	Prioritizing delivery of social and environmental benefits rather than economic profit maximization, through close integration between the firm and local communities and other stakeholders	improving the economic position of farmers and to increase transparency for the buyers by removing actors from the supply chain	helps farmers to increase or free up their working capital. The additional working capital may be used to invest in sustainable practices much as in the "develop scale-up solutions" from (Bocken et al., 2014).
- Aligning supply and demand - Improving through transparency - Data-driven farm optimization - Knowledge sharing	- Farming on food waste - Valorising farm waste - Marketing blemished and surplus food	- Farming equipment as a service - Farming as a service	- Transparent farming practices	- Payments for eco-system services	- Collaborative food processing - Online B2B marketplace - Online B2C marketplace	- Parametric insurance - Collaborative financing

[176] https://ploutos-h2020.eu/

To ensure farmers can 'call the shots' in their own operation, a concept known as control point[177] is useful. Examples of control points are access to data, terms of service, prices etc. The way these control points can or cannot be controlled by farmers affects whether net value for farmers is created or extracted. E.g. the JoinData[178] initiative has adopted the principle that farmers own their data and determine who gets access to their data.

3.4 Smart Production

The digitalisation of products, manufacturing processes, value chains and business models are the main drivers in the renewal of manufacturing companies. New data-driven services and business models cause disruptive changes in this domains (e.g. online stores, Airbnb types of platforms for manufacturing).

Promising innovation areas
The realization of Smart production is based on the following promising innovation areas such as[179]:

- Digitalisation, automation and robotization of production processes, cloud and IoT based;
- Digitalisation of value chains: demand/customer-driven flexible manufacturing processes, cloud and IoT based;
- Flexible, small-scale production in 'series of one' (mass customization)
- Predictive maintenance: advanced maintenance and repair;
- Development of new data-driven services and (mobile) platforms: data-driven business models.

Benefits, challenges in the context of digital sovereignty
Digitalisation and the underlying innovation areas have various benefits since 5G connectivity will make factory equipment even more connected and more industrial data will be generated and collected in the future.[180] Robots will be real time activated by artificial intelligence, allowing them to collaborate more to improve the work, safety, productivity and well-being of employees. Thanks to digital twins and Big data manufacturers can improve predictive maintenance and, based on consumer needs produce without inventories. Improvements around predictive maintenance stimulates new servitization based business models. The hyperscaler model, which is common for many of the current cloud- and data platforms, is also stimulating the take-up of servitization business models. But it will also entail challenges: since these (cloud)platforms might create lock-in effect caused by the powerful position of the platform. This can lead to a situation in which the platform is dictating the rules for the digital and physical part, resulting in a lack of (digital) sovereignty of the platform users.

[177] Eaton, Benjamin D., S. M. Elaluf-Calderwood, and Carsten Sørensen. "A methodology for analysing business model dynamics for mobile services using control points and triggers." *2010 14th International Conference on Intelligence in Next Generation Networks*. IEEE, 2010.
[178] https://join-data.nl/en/
[179] Bakker et al. Kansrijke Innovatie opgaven voor Nederland, (2017) TNO report https://publications.tno.nl/publication/34623505/7RjMww/bakker-2017-portfolioanalyse.pdf
[180] https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52021DC0118&from=de

3.5 Smart Security & Cybersecurity

Safety and security of our society concerns a number of things[181]; This mainly has to do with the protection of our critical infrastructure: dikes, bridges, roads, the gas and electricity grid, the sea and airports and our digital infrastructure. This concerns dealing with internal and external threats and instability. Crime, radicalization and (cyber)terrorism require an effective approach and innovations. Digital security such as cyber security and the protection of citizens is becoming an increasingly prominent issue that requires an integrated approach from government, companies and citizens.

Promising innovation areas
Promising innovation areas to come to a secure society are[182]:

- Secure and reliable physical and digital infrastructure;
- Security, privacy and identity of citizens: for example the use of Big data for a safe society (including risks and ethical questions);
- Preventing and dealing with radicalisation and terrorism: Technologies such as Big data analytics, Sensors and Advanced tracking and tracing technology offers great potential in identifying terrorism and radicalisation. To get the right information from the digital domain algorithms are needed.

Benefits, challenges in the context of digital sovereignty
Digital sovereignty plays an important role in a secure society. In the light of the sovereignty of citizens the benefit is that with the emergence of these aforementioned digital technologies, citizens are protected against threats. The involved challenge concerns the privacy and identity of citizens. New laws and regulations regarding privacy, data storage and access must guarantee security.

3.6 Smart Society

Our society develops and changes continuously in terms of population, immigration, urbanization, economy and technology and call on the adaptive capacity of our society. A resilient society is about social cohesion and polarization. The population dynamics in the Netherlands and Europe, with growth and shrinkage in various regions, ask for 'smart' solutions to keep cities livable and, in the countryside, facilities affordable and accessible. It is for instance a continuous task to keep a (shrinking) working population fit for (future) economic activities in the digital age. Some jobs will disappear, and new professions arise. At the same time the composition of households is changing (smaller size, larger number) and require adjustments to our living environment to ensure adequate planning and development of smart homes. Within smart homes; automation systems will monitor and control home attributes such as lighting, climate, and appliances (e.g. to better manage our increasing energy demand). It may also include home security (e.g. access control and alarm systems). When connected with the Internet, home devices are an important element of the Internet of Things.

[181] Bakker et al. (2017), Portfolio kansrijke innovatie opgaven voor Nederland. TNO report.
[182] Ibid

Promising innovation areas
The aforementioned digitalisation of society will be enabled by promising innovation areas such as[183]:

- Knowledge and skills for the digital age (smart skills, e-skills, human-machine interaction);
- New arrangements for working in the digital society (smart working);
- Smart houses and neighborhoods for a diverse population.

Benefits, challenges in the context of digital sovereignty
Promising innovation areas such as building smart houses also provides solutions for societal challenges such as the increasing energy demand. We will illustrate this based on the Interconnect project. The project is also used to show benefits and a challenge in the context of digital sovereignty. In response to our ever increasing energy demands, the Interconnect project[184] is an example of an initiative focusing on improving energy management for end-users, enabled households based on smart systems and energy management solutions and grid-based systems. To ensure that the project can establish cross-country impact in Europe, the consortium has been working on the SAREF ontology – a reference architecture that standardises the interfaces to devices, appliances and sensors facilitating semantic interoperability between them. Accordingly, the energy utilization and consumption of appliances can be interconnected, facilitating end-users (through the use of integrated platforms) to make decisions on a system or household level rather than on individual appliance. This provides benefits by enabling end-users to optimise their energy usage (in collaboration with grid operators). The development of the shared SAREF ontology is key: with different vendors and types of appliances across Europe, decentralised solutions would results in disjointed or disconnected energy management solutions. Alternatively, in case a universal standard is developed by a single large scale player in the market, this would create a monopolistic scenario in which all grid operators or solution providers would depend on this single player, which would mean a challenge in terms of sovereignty. Therefore, the European Union has pushed for the development of a shared ontology that can be leveraged to make appliances in households interoperable, as well as facilitate the establishments of energy management systems and solutions that can also span the boundaries of countries – in fact, a lot of appliance providers already offer products in many countries, making such a shared standard even more attractive to pursue.

[183] Bakker et al. (2017), Portfolio kansrijke innovatie opgaven voor Nederland. TNO report.
[184] https://interconnectproject.eu/

4. Scenarios related to digital sovereignty

As described in Chapter 2 the Netherlands and Europe are highly dependent on non-European countries on almost all digital technology layers. This dependency is also illustrated by the six domains in Chapter 3. Ultimately, it is a question of which interests the Netherlands and Europe must safeguard to maintain or create capacity to act globally. [185] In this chapter we describe four scenarios of the capacity to act and the level of digital sovereignty.

The four scenarios are based on two drivers relevant to act global:

- The first driver concerns **international cooperation** among foreign partners, which can be strong or weak. *Strong cooperation* is based on frequent reciprocity among foreign parties, and complementarity and interoperability among their digital technologies. *Weak cooperation* is characterised by very limited or no reciprocity among foreign parties, and lack of complementarity and interoperability among their digital technologies.
- The second driver is **ease of trade** among foreign partners, which can be low or high. This concerns the ease of doing business among international partners. The world bank even developed a raking for the ease of trade (called the ease of doing business) based on parameters such as regulations for businesses and protection and property rights. In case of an open economy in which foreign parties can execute trade activities without restrictions (e.g. without high import duties) the ease of trade among foreign parties is *high*. In case of protectionism the ease of trade is *low*.

Based on these two drivers the four scenarios can be presented as follows (see Figure 8).[186]

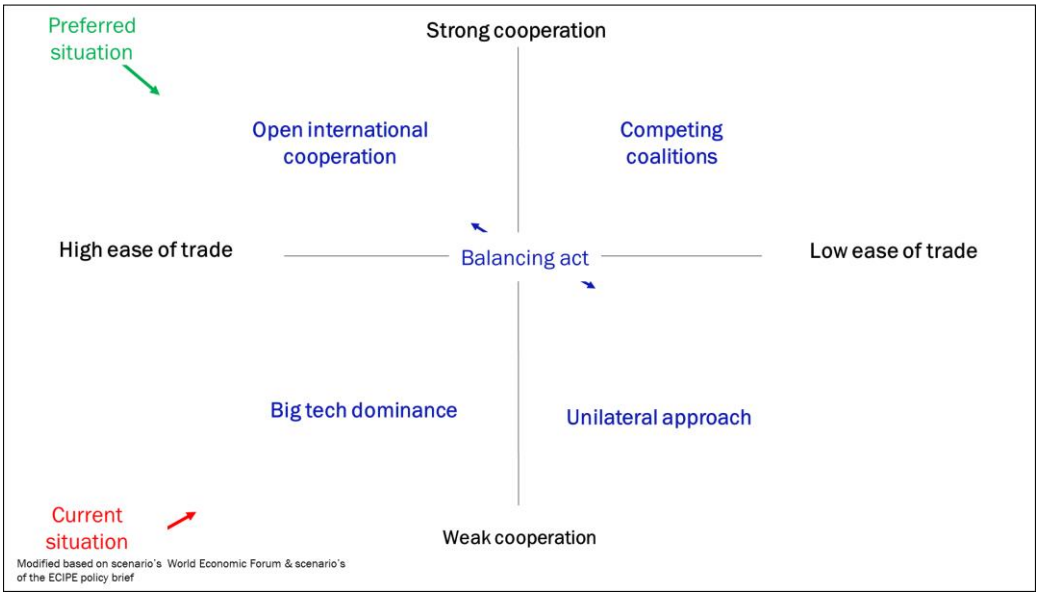


Figure 8. Four scenario's related to digital sovereignty[187]

[185] https://hcss.nl/report/soevereiniteit-en-digitale-autonomie/
[186] Partially based on: https://www.weforum.org/agenda/2019/01/four-future-scenarios-for-trade-and-investment-which-one-will-win/
[187] Ibid

4.1 Scenario 1 Open international cooperation

Scenario 1, called Open international cooperation, is the preferred scenario since this scenario provides the best chances for a level of digital sovereignty that preserves Europe's societal values and social market economy (e.g. in terms of international cooperation and trade).

In the preferred scenario[188], foreign parties come together to cooperate based on complementary digital technologies and interoperability, and trade flows move easily across borders. Major economies jointly commit to address points of conflict and collaborate to revitalize the WTO through 'plurilateral' negotiations, with significant contributions from both advanced and emerging economies. On global level actions are taken on major issues: modernising trade rules; minimising distortions created by unfair subsidies; governing digital trade; strengthening the WTO's monitoring and dispute settlement functions.

Public and private stakeholders also cooperate to strengthen mechanisms for investment governance across different international platforms. Likewise, trade policymakers build cooperative mechanisms with other policy communities on relevant issues such as data flows, cybersecurity, laying coherent global governance foundations for innovation, growth and productivity gains.

In this scenario the Netherlands and Europe are substantially investing in the digital infrastructure and are leading in setting standards.

4.2 Scenario 2 Competing coalitions

In the Competing coalitions[189] scenario, foreign parties cooperate, but much of it is influenced by emerging deep structural rifts over the role of the state in governing data flows, investment and advanced industrial and digital technology that holds national security applications.

Amidst these differences, trade and investment flows are directed by political intervention rather than price signals, and pressure comes to bear on multinationals to restructure and localize value chains. It becomes impossible to make progress within the WTO and multilateral governance is supplanted due to closed regional blocs. Heightened concerns over the geopolitical and security implications of investment result in the bifurcation of investment flows (China versus the US, the EU). Some regions – such as the US and China vs Europe – and global businesses become caught in between different spheres of influence. In a zero-sum dynamic, individual countries stakeholder come under pressure to lean towards one bloc over another, with negative repercussions for geopolitical stability, economic development and global governance. These geopolitical dynamics will likely result in a global competition between US, China and Europe on who becomes most digital sovereign.

In this scenario the Netherlands and Europe mainly invest backward in the digital infrastructure on a fragmented basis.

[188] Partially based on https://www.weforum.org/agenda/2019/01/four-future-scenarios-for-trade-and-investment-which-one-will-win/
[189] Ibid

4.3 Scenario 3 Big Tech dominance

The third scenario is called Big Tech dominance.[190] This is the scenario in which we currently are, foreign non-European parties act unilaterally rather than cooperatively, but innovation of digital technologies races ahead of regulation. There is lag of interoperability and technological complementarity limiting a cooperative approach among foreign parties.

A borderless world is created for some, while others face wide-spread uncertainty and inefficiencies. Firm-led disruption creates pockets of radical innovation with the potential for winner-take-all profits. This leads to a high ease of trade, for large non-European Big Tech firms that are based on 'hyperscaler' based business model. Small and medium sized enterprises, however, become in an unfortunate position by high barriers to entry in some technologies and greater fragmentation in the global economy. While first-mover benefits in any given industry might be out-sized, these advantages combined with the lack of strong global intellectual property (IP) protection norms generates incentives for theft and other forms of economic espionage. Fragmented regulatory frameworks for data flow governance raise cybersecurity risks and increasing costs. Investment flows that are dependent on long-term predictability are likely to be dampened. Small businesses and consumers in weaker economies might lose access to the latest digital technologies and services. Conflicts between governments may also increase. Without multilateral options for rules-based dispute resolution, differences will be settled on power considerations, generating yet more uncertainty and increasing business costs. This results in a situation in which Europe has a low level of digital sovereignty compared to the US and China.

In this scenario the Dutch and European investments in digital technologies are low compared to other non-European countries and the focus of Europe is mainly on regulation.

4.4 Scenario 4 Unilateral approach

This fourth scenario, Unilateral approach[191], is the worst-case scenario. In this scenario unilateral action and a high frequency of economic conflict leads to a normalization of trade wars between major economies (e.g. the US and China). Trade and investment issues become political weapons in broader geopolitical competition. In this scenario the US, China and Europe all have a high level of digital sovereignty at the expense of a low ease of trade and limited international cooperation.

The uncertainty and instability associated with entrenched economic conflict drains investment flows and business confidence. Without investment and facing high barriers to knowledge exchange, firms cannot innovate or develop digital technologies. Deep disruptions occur in global value chains, potentially leading to reshoring or de-globalization. The global economy slides into protracted decline, creating major domestic challenges for most countries and foreign parties. These challenges include higher costs for consumers and rising unemployment, as well as

[190] Partially based on https://www.weforum.org/agenda/2019/01/four-future-scenarios-for-trade-and-investment-which-one-will-win/
[191] Ibid

domestic unrest. As major powers turn inwards to deal with domestic crises, populist and protectionist sentiments drive up the risks of international conflict. Limited options for orderly dispute resolution at the international level deepen the risks of long-lasting economic decline.

Dutch and European policies in this scenario encourage digital bonding within EU by taking a defensive position against the outside world.

These scenarios have been drawn to sharpen the risks and trade-offs involved of the current scenario, preferred scenario and the other scenario’s.

5. Key issues

The Netherlands and Europe are currently in the Big Tech dominance scenario when it comes to digital sovereignty. In this Chapter we describe the key issues related to this scenario. These issues needs to be solved to come to the preferred scenario: the Open international cooperation scenario. These key issues are composed based on a literature study and expert interviews. All selected key issues are equally important, meaning that their order of description does not imply that the first key issue is more important than the second key issue for instance.

5.1 Large one-way dependency / lack of reciprocity

Although the current scenario provides a high ease of trade, it limits cooperation based on reciprocity. Since there is a large one-way dependency on an increasingly small number of providers of digital technologies. This is the case for most digital technology layers, especially for the data infrastructure and cloud layer, having a 'hyperscaler' business model. We also see that many of these providers are located outside of Europe. That means that the competitiveness of the EU digital space has become questioned (see Appendix G for more details on the economic impact).

5.2 Lack of respect of European values

It is very challenging in the current scenario to protect public European values such as:

- Intellectual property; Besides systematic theft of intellectual property of our knowledge intensive firms by various stakeholders worldwide[192], Big-tech do not respect the intellectual property of smaller players.[193, 194] There is for instance growing number of patent disputes over cloud-related applications.[195] Most smaller companies are less experienced with legislation and patent legislation compared to big-tech who can afford the best and more legal advisors.[196] That increases the chance for smaller companies to lose intellectual property disputes.
- Privacy[197]; Sometimes, although not always, websites, platforms and applications ask users to check boxes indicating that they have read and agreed to the privacy policy. This framework assumes things that are not true:
  - That users read privacy policies;
  - That the users understand what the policies say and;
  - That users have a practical choice about whether or not to use a website or application under those conditions.

  Since these assumptions are wrong, the "notice and choice" framework simply can't protect privacy.

[192] Moerel, Timmers (2.0) - Preadvies Staatsrechtconferentie 2020.pdf (uu.nl)
[193] https://www.cato.org/regulation/spring-2021/why-big-tech-likes-weak-ip
[194] https://techcrunch.com/2021/11/01/is-big-tech-bad-at-business/
[195] https://kvdl.com/artikelen/octrooigeschillen-cloud-volgende-stap
[196] Ibid
[197]https://publicknowledge.org/the-privacy-debate-reveals-how-big-techs-transparency-and-user-control-arguments-fall-flat/

- Dis-and misinformation; The role of large social media platforms as privileged providers of online disinformation became evident during the US Presidential elections, the Brexit referendum of 2016, and many other events thereafter.[198]

5.3 Data ownership and data sovereignty issues

In the current scenario most European data is stored either outside of Europe[199] or, if it is stored in Europe, on servers belonging to non-European companies. Subsequently companies and citizens are often unsure who owns their data and that constitutes a major obstacle to the sharing of data and the availability of this data for future value creation. Some specific issues also need to be addressed such as the ownership of sensor data where the question is if ownership and copyrights rest with the company that produces the sensor data (the user) or with the manufacturer of the sensor (the supplier).[200] Legally data ownership does not exist at the moment as it is undefinable as a good.

5.4 Cloud issues/ infrastructural issues

In the current scenario the biggest threat is the potential Monopoly, that is based on the fact that cloud services (the centralised architectures) are provided only by a few US (Google, Microsoft Azure, Amazon Web Services) and Chinese based suppliers (Alibaba cloud).[201] There is a limited number of European providers.[202] Many companies are considering to use cloud services to replace their in-house data infrastructure for sharing and analysing data (IoT, administrative data, etc.).[203]

In the recent past the market penetration of cloud services was relatively low, but this is a rapidly changing landscape. In the period 2014-2018, the big three cloud providers still had a very small market share of different types of software.[204] Yet they are rapidly increasing their market share in different types of software, especially in system infrastructure software and application development and delivery.[205] That means that these cloud providers are vertically integrating services and extending their role in other market segments.

5.5 Security concerns

Security concerns in the current scenario are directly related to cybersecurity concerns (e.g. the ransomware attack that took down Garmin cloud services[206], or the cyber-attack of VDL[207]). Cyber-treats and attacks are increasing[208] and are

---

[198] https://www.medialaws.eu/rivista/regulating-big-tech-to-counter-online-disinformation-avoiding-pitfalls-while-moving-forward/
[199] https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/
[200] Gijsbers et al. (2020) Envisioning the Industrial B2B platform economy, TNO report TNO 2020 R12278
[201] Gijsbers et al. (2020) Envisioning the Industrial B2B platform economy, TNO report TNO 2020 R12278
[202] Ibid
[203] Ibid
[204] McKinsey and Company (2020) The next software disruption: How vendors must adapt to a new era. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-next-software-disruption-how-vendors-must-adapt-to-a-new-era
[205] Ibid
[206] Garmin confirms ransomware attack took down services | TechCrunch
[207] https://www.vdlgroep.com/en/news/vdl-groep-back-in-business-after-cyber-attack
[208] Moerel, Timmers (2.0) - Preadvies Staatsrechtconferentie 2020.pdf (uu.nl) (in Dutch)

mainly coming from non-European countries such as China, Iran and Russia who have offensive cyber-attack programs for instance against the Netherlands.[209] New technologies such as AI makes it even easier to carry out cyber-attacks, because existing vulnerabilities can be discovered and exploited automatically and on a large scale.[210] Additionally, while adopting innovative ICT such as artificial intelligence, the mere usage of AI itself creates a bigger attack surface.[211]

Other security issues relate to artificial intelligence such as biased algorithms, privacy-violating facial recognition systems and autonomous vehicle accidents caused by dangerous unintended consequences of AI.[212]

5.6 Lack of interoperability and data portability

Interoperability is too limited in the current scenario (e.g. various 5G suppliers applying their own interfaces).[213] This reduces flexibility in switching to current and future standards (e.g. 5G, 6G) and limits data portability (the opportunity to move data to another cloud or data storage infrastructure). Interoperability is key to communication among stakeholders within the preferred scenario –Open international cooperation. Interoperability enables reciprocity since it determines the ability of systems, products or devices to connect, communicate and cooperate. Standards ensure interoperability and seamless communication between actors and systems. Standards, when adopted substantially, are very powerful economic and innovation assets. They can be private such as the Apple standards or they can be public such as the GSM standard.[214] Some private standards are tightly controlled (such as Apple) while others, such as the public and open source Linux standard develop in different directions.[215] Standards are important to support modular development, avoid fragmentation, avoid vendor lock-in and ensure a level playing field.

5.7 Lack of skills and capabilities

The Netherlands and Europe are lagging behind with their digital talent in the current scenario.[216] Digital skills and capability development are a key topic to the digital transformation (e.g. for value chains, companies, and citizens) and to enable the development of alternatives to the current dominating non-European digital technology solutions. Skills development include hard and soft skills for the entire workforce including vocational training.[217] With an ageing workforce in the Netherlands and Europe retraining of staff at all levels becomes important [218]; It

[209] https://www.nctv.nl/documenten/publicaties/2019/6/12/cybersecuritybeeld-nederland-2019
[210] CSR Advies Nieuwe Technologieën.
[211] Herpig, Sven. (2019). Securing Artificial Intelligence Part 1: The attack surface of machine learning and its implications.
https://www.researchgate.net/publication/341792988_Securing_Artificial_Intelligence_Part_1_The_attack_surface_of_machine_learning_and_its_implications
[212]https://www.cmswire.com/information-management/responsible-ai-moves-into-focus-at-microsofts-data-science-and-law-forum/
[213] Based on expert input
[214] Gijsbers et al. (2020) Envisioning the Industrial B2B platform economy, TNO report TNO 2020 R12278
[215] Ibid
[216] Organisation for economic co-operation and development: Skills Outlook,
https://www.oecd.org/education/oecd-skills-outlook-e11c1c2d-en.htm
[217] Gijsbers et al. (2020) Envisioning the Industrial B2B platform economy, TNO report TNO 2020 R12278
[218] Ibid

requires a reconsideration of the roles of different actors in the education system, industry organization, vendors and companies. Especially, SMEs have limited resources for training . An alternative to skills development and investing in European talent is acquiring more non-European talent. But this second solution means that Europe becomes also on skills level dependent on non-European countries.

The negative impact of these key issues (economic, innovation and societal impact) is described in Appendix G.

6. Towards the preferred scenario

There are a number of measures recommended to realising the preferred scenario. They fall into three main groups: technological solutions, policy solutions (including regulation and standardization) and business model solutions (including organizational models and value chain arrangements). These measures are composed based on a literature study and expert interviews.

6.1 Technological solutions

Technological solutions are a key driver of digital sovereignty. We highlight the following solutions:

Focus on the development of 6G
The European Commission should support intensive research, via its innovation programs, in the field of 6G to create a strong position to become ready when the next development in mobile connectivity comes around.[219]

Build European cloud services such as Gaia-X
As soon as completed the European cloud service Gaia-X should become a viable solution to mitigate dependency on the big non-European cloud providers. What emerges with this solutions is not a cloud, but a networked system that links many cloud services providers together.[220] This solution should directly contribute to European digital sovereignty as the data stored via this initiative should not be subject to the US Cloud Act.[221] A number of countries besides the France and Germany which started the initiative are joining the Gaia-X effort. This resulted for instance in the set-up of Gaia-x hubs at country level in order to animate the Gaia-X communities locally (e.g. in the Netherlands, France, Germany etc).[222] The Gaia-X hub in the Netherlands is initiated by TNO and its partners, with the support of the Ministry of Economic Affairs and Climate. Stimulation by the European Commission and Member states is needed for a broad uptake of this initiative in Europe.

Become a frontrunner in Edge computing
Europe must position itself more broadly as a frontrunner in the edge computing domain to gain first-mover advantage and avoid falling behind, like it has on other technology layers. This requires focused R&D investments by the European Commission, the Netherlands and the industry.

Develop decentralised data infrastructures
The broad availability of distributed / decentralised platform infrastructures will be a key condition for realising the preferred scenario (Open international cooperation). Such systems are more complicated than centralised systems and databases in the hands of Big Tech.[223] Several initiatives are underway to build such federated systems, but their full development and implementation will take some years[224] and

[219] https://dgap.org/sites/default/files/article_pdfs/210422_report-2021-6-en-tech.pdf
[220] https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html
[221] Gijsbers et al. (2020) Envisioning the Industrial B2B platform economy, TNO report TNO 2020 R12278
[222]https://events.talque.com/gaia-x-summit/en/6iq6yI5LPSxaIRA6cmnq?talque=lecture-list&lectureId=nYBjbRFFuIr8fmLUM5iJ
[223] Gijsbers et al. (2020) Envisioning the Industrial B2B platform economy, TNO report TNO 2020 R12278
[224] Gijsbers et al. (2020) Envisioning the Industrial B2B platform economy, TNO report TNO 2020 R12278

require further stimulation by the European Commission and Member states. One example is the aforementioned Industrial Data Spaces (IDS) which aims to create a decentralised *"virtual data space in which partners in business ecosystems can securely exchange and easily link their data assets. The main goal of the International Data Spaces is to facilitate the exchange of data between Data Providers and Data Users"*[225]

Develop and adopt open technology and data standards
The technology community is recommended to develop and adopt open technology and data standards for data sharing and analysis etc. Closed and proprietary standards and software are key obstacles to move from the current scenario in to an Open international cooperation scenario. Open standards (e.g. Linux based) are becoming more common and important to ensure interoperability and portability of data among (cloud)platforms. Open standards also lower the barriers to enter the market and platform domain, especially for SMEs (who form a large group in the European Industry).

Develop interfaces to provide easy access
The technology community is recommended to develop easy to find and use software and interfaces, complementing to the aforementioned standards. [226] This is important for companies to come to the preferred scenario (Open international cooperating), especially for smaller companies.[227]

Focus on R&D for future technology paradigms such as quantum technology
A persistent and substantial investment in future technologies (e.g. next generation ICs, batteries and antennas, cryptography and quantum technology) by the European Commission, the Netherlands and the industry is needed to ensure the EU's sovereignty and technological competitiveness. This also means fostering innovation via public-private partnerships by both public partnerships.

6.2 Policy solutions

Policy solutions are required to strengthen the technological solutions. These policy solutions mainly require a facilitator role and a regulator role from the government. We highlight the following;

As **facilitator** the government is recommended to:

Support the development of (open) standards and impose those standards
A key public responsibility on European level is to support the development of (open) standards and imposing those standards, such as in the case of the GSM standard to move to the preferred scenario. Standards should be developed by the technology community in consultation with companies and regulators to ensure that they contribute to interoperability, data portability and a level playing field, while avoiding adoption problems due to a 'battle of the standards'.[228]

[225]https://www.fraunhofer.de/content/dam/zv/en/fields-of-research/industrial-dataspace/whitepaper-industrial-data-space-eng.pdf
[226] Gijsbers et al. (2020) Envisioning the Industrial B2B platform economy, TNO report TNO 2020 R12278
[227] Ibid
[228] Gijsbers et al. (2020) Envisioning the Industrial B2B platform economy, TNO report TNO 2020 R12278

Promote a level playing field
To move out of the current Big Tech dominance scenario a level playing field needs to be promoted by the European Commission through the stimulation of cooperative platform models. Such models provide access to all types of users (e.g. small and large firms, services providers, customers and suppliers). The Smart Connected Supplier Network (SCSN)[229] initiative is an example of such a model. The partners of the Smart Connected Supplier Network (SCSN) initiative developed a standard for information sharing based on semantic technology, thereby ensuring optimal interoperability between the supply chain partners for the most prominent information streams.[230] The SCSN standard builds on the aforementioned International Data Spaces (IDS) standard. SCSN and IDS bring a "connect-once - reach the entire value chain scenario" to the supply chain.[231]

Remove obstacles and barriers for data sharing
Economic incentives, legal clarity on who can do what with the data and contractual agreements, are recommended to apply by the industry to stimulate data sharing and better training of AI systems.

Provide skills development policies
Providing skills development is an important function of the public sector (e.g. European Commission and the Netherlands) to orchestrate and provide training functions at a number of levels for different age groups on a wide variety of technological (hard skills), business and social aspects (soft skills).[232]

As **regulator** the government is recommended to:

Develop laws and regulations to protect norms and values
Europe should strengthen its global reach in the regulatory domain to protect European norms and values, by making legal instruments capable of extending their application on global level; the aforementioned GDPR is a good example.

Besides that it is important that the EU provides clarity on who has ownership of and access to different types of data, such as those provided by sensors.

Provide cybersecurity, rules and regulations
Providing cybersecurity requires a mix of:
- Stimulation of the European Commission to develop robust technologies processes and procedures by the industry;
- Laws and regulations developed by European regulators.

6.3 Business model solutions

Business model solutions are needed to bring the aforementioned technological solutions to the market and scale them. We recommend the following:

Apply a collaborative business model approach
The European Industry and service providers are recommended to apply a collaborative business model approach for European digital technologies that

[229] https://smart-connected.nl/
[230] Stolwijk C., and Berkers F., (2020) Scalability and agility of the Smart Connected Supplier Network approach; http://publications.tno.nl/publication/34637132/HajIaR/TNO-2020-R11179.pdf
[231] Ibid
[232] Gijsbers et al. (2020) Envisioning the Industrial B2B platform economy, TNO report TNO 2020 R12278

require “roll-out” or “institutionalization” (e.g. distributed / decentralised platform infrastructures). A market transformation is proposed based on ‘adding” sustainability practices (as voluntary sustainability standards) to “business as usual”. This transformation contains four stages[233] (see Figure 9).

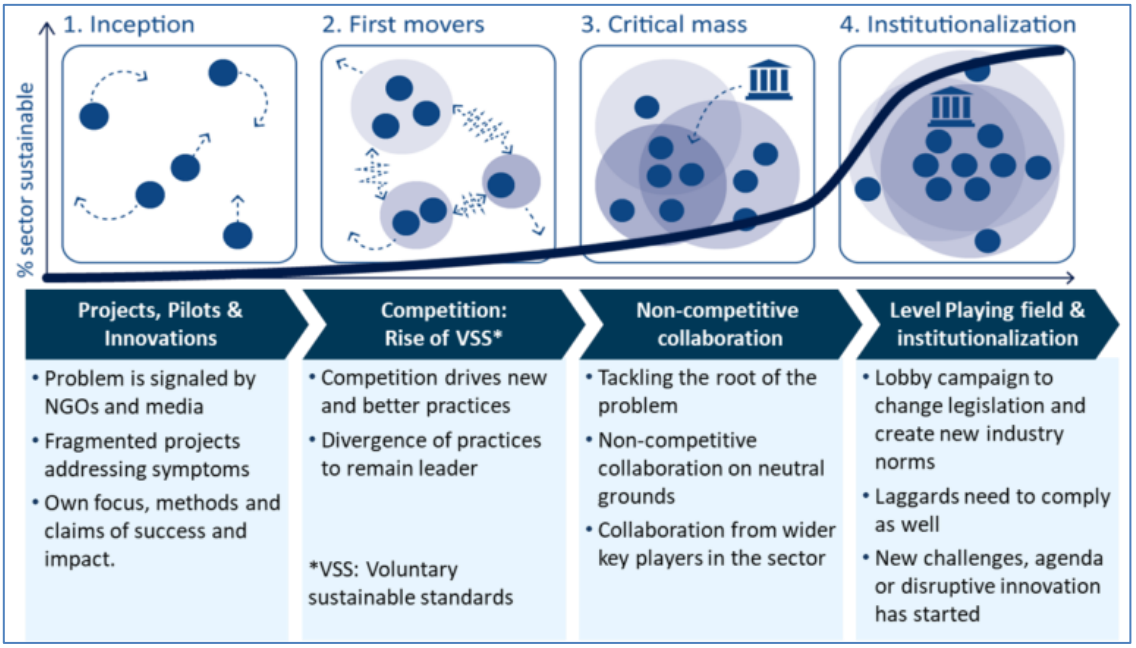


Figure 9. Model of sustainable market transformation[234]

After piloting the new digital technologies in the 1nd phase, the 2nd and 3rd phase are crucial in achieving a novel sovereign common practice. In the 2nd phase real-life businesses and value networks[235] have adopted a specific novel way of working. We see this approach for instance in various European data sharing practices (e.g. iShare[236], SCSN[237], JoinData[238]). They all have their specific standards, ‘couleur locale’, and members that are actually frequently sharing data and are important for the scale effect. In the 3rd phase non-competitive collaboration is required. The involved partners identify what is working properly and run into trouble having to meet different sets of standards (e.g. many couleurs locales). That implies that the partners need to focus on their commonalities (e.g. concerning data sharing initiatives and standards). This however requires substantial coordination and interoperability, but it creates a strong value proposition for “full roll-out” or “institutionalization”. An alternative pathway is to establish a smaller value proposition with less partners. Once this deployment is initiated, additional partners extend the value proposition (based on a kind of snowball approach). This alternative approach has less risks, as from the initial launch, value has already been created. Figure 10 depicts different pathways of achieving full rollout. The

[233] Simons, Lucas, and André Nijhof. Changing the Game: Sustainable Market Transformation Strategies to Understand and Tackle the Big and Complex Sustainability Challenges of Our Generation. Routledge, 2020.
[234] Ibid
[235] Value chains that turned in to networks enable by digitalisation
[236] https://www.ishareworks.org/en
[237] https://smart-connected.nl/over-scsn/stichting-scsn
[238] https://join-data.nl/en/about-joindata/

most optimal path for full “full roll-out” or “institutionalization” is probably in the middle.

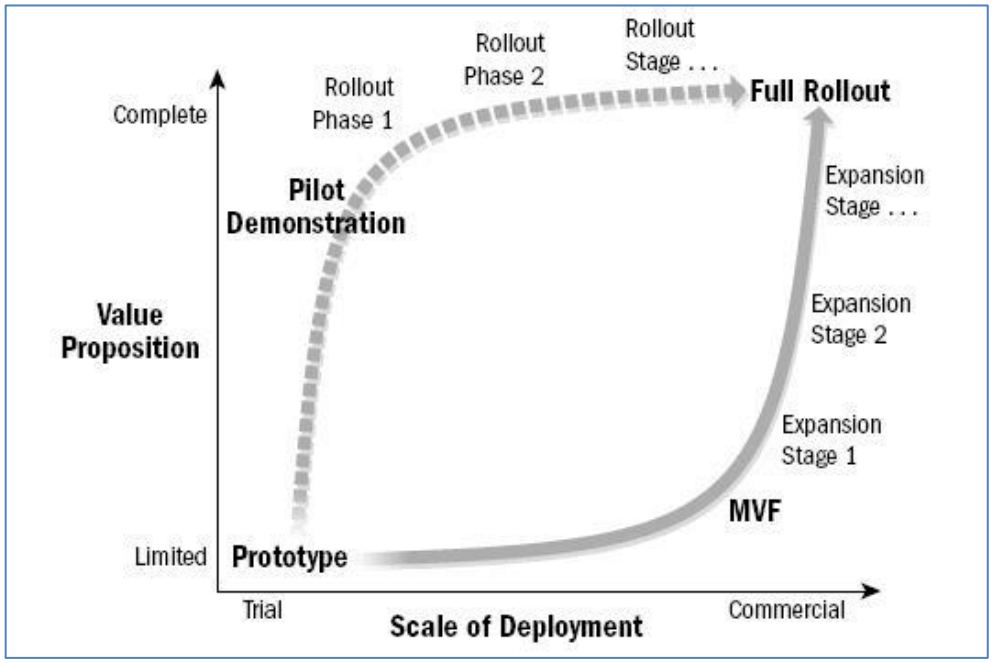


Figure 10. Pathways of achieving full rollout [239]

Apply user-oriented business models

Platforms are recommended to apply user-oriented business models to avoid users becoming too dependent on the platform for value creation.[240] These business models are enabled by providing an infrastructure and tools that facilitate the matching processes among platform users and also to stimulate the innovation of value adding applications on top of the transactions taking place over the platform.[241]

Stimulate governance and membership models

Membership models are recommended to value chains that want to digitalise to distribute digitalisation costs between suppliers and users in a value chain.[242] The membership model may also be used to provide preferential access to SMEs using a type of freemium model for cross-subsidising. Pricing mechanism, such as reduced fees for SMEs will lower the threshold for their participation. Such a membership model requires a clear governance (e.g. based on a foundation that distributes the costs between the members). Governance is also needed to safeguard the collective value of the digitalisation and to balance the power between larger and smaller participants. A governing body is crucial to manage the standard to enable the communication in the value chain, but also to promote wider adoption of the standard and the network’s proposition. In other words, to manage the network effects of the coalition’s joint business model.

[239] Adner, Ron. The wide lens: A new strategy for innovation. Penguin Uk, 2012.
[240] https://www.government.nl/documents/reports/2019/10/07/digital-gatekeepers
[241] Gijsbers et al. (2020) Envisioning the Industrial B2B platform economy, TNO report TNO 2020 R12278
[242] Ibid

6.4 The role of applied research

In this section we also discuss our own role as applied research organization to increase the digital sovereignty and enable the preferred scenario.

Applied research acts as an intermediary between fundamental research and its application in business and society. Organizations for applied research, RTOs (Research & Technology Organizations), produce, integrate and transfer science and technology to help resolve grand challenges and support industrial competitiveness. They can do this in several ways:

- Through **technological development**, increasing the TRL (Technology Readiness Level) of new, potentially disruptive, technologies through research.
- By acting as a **neutral intermediary** between technology providers and/or users. In some cases a more involved role is possible as well, if this serves the purpose.
- By providing **consultancy and advice** to governments and industrial stakeholders.

Our applied research organization, TNO, develops innovations that can increase the digital sovereignty of the Netherlands and Europe on various parts of the technology level model (see Figure 11). The unit ICT of TNO is doing that on the core of the model (the blue layers from network and connectivity, till applications presented in Figure 11) based on the roadmap digital innovations. The roadmap digital innovations has four focus areas[243]:

1. Fast and open infrastructures: *"to make a difference in a generic, highly flexible ICT infrastructure that delivers instantly and ubiquitously accessible ultrahigh bandwidth connectivity, massive storage and processing as well as application platforms that adapt to utilize the available resources optimal".*
2. Data sharing: *"to enable data sharing opportunities for Dutch and European stakeholders (e.g. firms) based on controlled access to available data, data interoperability, digital validation of information and reliable analysis of data".*
3. Embedding systems innovation: *"to make a difference in the High Tech industry by addressing the challenge of mastering architecting and design of ever increasing complex systems through new and radically improved systems / software and engineering methods".*
4. Trusted ICT: "*to prevent risk of financial loss, disruption or damage to the assets and reputation of organizations from some sort of failure of its information technology systems. Relevant focus areas to enable trusted ICT are automated security, monitoring and detection, quantum safe technology and resilience engineering."*

The unit Industry of TNO is enabling digital sovereignty based on its activities presented on the left and right side of the model. The unit Strategic, Analysis and Policy of TNO is supporting these activities based on its expertise about policy instruments (including financial instruments and regulation), business model expertise for market applications of digital innovations, orchestrating innovation expertise to set up public private partnerships to enable digital innovations and its expertise about underlying materials and sourcing. The unit Circular Economy & Environment also addresses this field of underlying materials.

[243] Roadmap Digital Innovations TNO

The other six units of TNO (Building, Infrastructure & Maritime, Healthy Living, Traffic & Transport, Circular Economy, Safety and security and Energy Transition) are active in the verticals in which these technical levels are applied and contribute with their domain specific expertise.

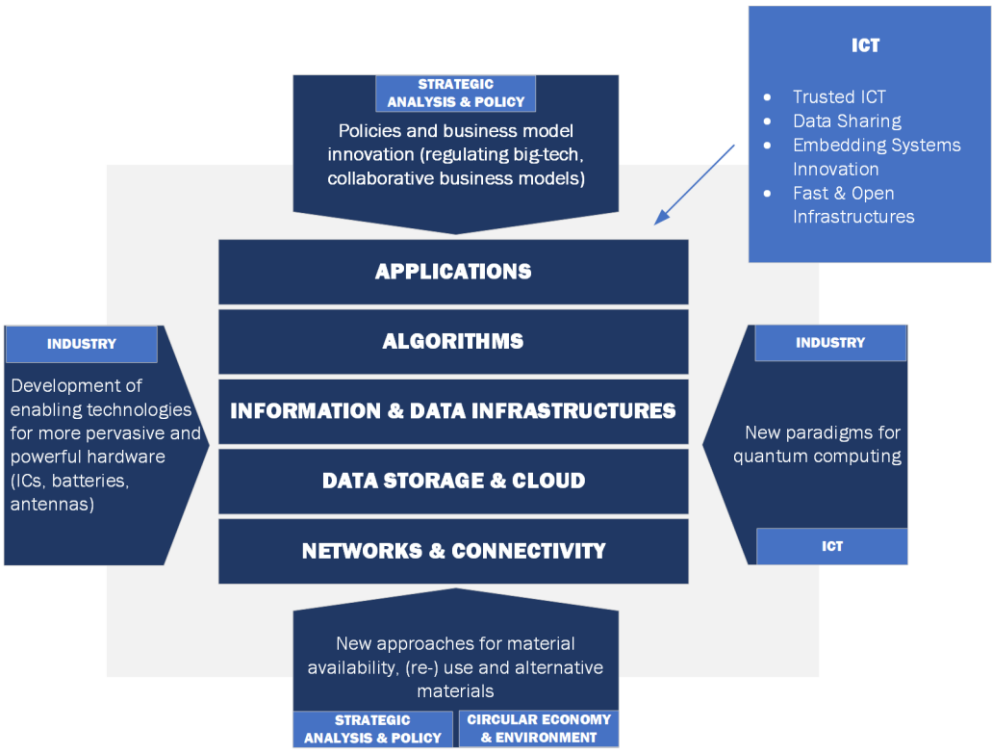


Figure 11. The role of TNO on the various layers of the Technology level model

Promising innovation areas for TNO to increase the digital sovereignty are:

- Development of 6G.
- Development of European cloud alternatives.
- Development and increasing market applications of decentralised data infrastructures based on a collaborative business model approach.
- Developments on edge computing fits to the expertise of the unit ICT.
- R&D related to future technology paradigms (e.g. next generation ICs, batteries and antennas, crypthography and quantum technology).
- Advice on (global) laws and regulations to protect norms and values (e.g. to protect the privacy of platform users).

These areas build on the aforementioned solutions described in the previous sections. TNO is already active on most of them.

7. Concluding summary

7.1 Meaning and importance of digital sovereignty

In this paper we indicate that digital sovereignty means the control over the design and use of digital technologies. Digital technologies have a major impact on how our society and economy functions. During the pandemic, for instance, it saved many sectors from a collapse by enabling teleworking from home; it can make production processes more efficient and there are a lot of cost savings involved, to name some advantages. However, the downside is that digital technology can have a detrimental impact when it is misused by those with bad intentions (e.g. big-tech not respecting the IP of smaller players, violating privacy of citizens, ransomware attacks etc.). This means that the less control the Netherlands and Europe have over digital technologies the more dependent we become on others, including those that do not share our values and those who are ill- intentioned. Moreover, a lack of digital sovereignty also leads to a decrease in competitiveness of the EU digital space. These, among other reasons, point to the importance of digital sovereignty to ensure the long-term preservation of European societal values and our social market economy.

7.2 Our Dutch and European position

In the paper we show that the dependence on non-European digital technologies for the Netherlands and Europe is currently at an unacceptable level, since a strong dependency is present on almost every digital technology layer;

- **Networking and connectivity;** The development of cellular network standards has shifted from Europe (for 2G, 3G and 4G) to Asia (for 5G), whereas in the past Europe had a leading role.
- **Data storage & cloud;** There is an increasing dependence on US-led hyperscalers (Amazon, Google, Microsoft). At the same time there are concerns about the impact on the US Cloud Act, which threatens the security of data stored in Europe. Decentralised European alternatives such as Gaia-X and IDS are under development, but not fully implemented yet.
- **Information & data infrastructures;** The layer of information and data infrastructures is also driven by non-European hyperscalers.
- **Algorithms;** The data pools that are enabling for algorithms and machine learning applications are in the hands of non-European stakeholders.
- **Applications;** The application layer is where the money comes from. However, the applications are often in non-European hands since the Netherlands and Europe are not sovereign on the underlying digital technology layers.

Besides that there is a strong non-European dependence on underlying materials and components.

However, there are also various **opportunities** for the Netherlands and Europe that require strong investments and relate to:

- Smaller, cheaper and more powerful hardware such as EUV for ICs, better batteries and antennas – enabling more pervasive computing.
- New paradigms for cryptography and quantum technology.

We present four scenarios concerning possible futures of digital sovereignty, including the current and preferred scenario. They are; **1. Open international cooperation, 2. Competing coalitions, 3. Big Tech dominance** and **4.Unilateral approach**. The scenarios vary based on the level of international cooperation and the ease of trade. Given the high dependence on non-European countries on almost every digital technology layer the Netherlands and Europe are currently in the Big Tech dominance scenario. That scenario is characterised by weak international cooperation and a high ease of trade for non-European Big Tech firms. The risk is to end up in the Competing coalitions scenario, which is based on deep structural rifts or the Unilateral approach scenario that is characterised by frequent economic conflicts. The preferred scenario is 'Open international cooperation', which provides the best chances for a form of digital sovereignty that preserves societal values and our social market economy.

7.3 Recommendations for an optimised Dutch and European position

The range of measures adopted by the Netherlands and Europe so far provides a first step. However, to move to the preferred scenario the Netherlands and Europe needs to be at the forefront of developing digital technologies. This requires a more proactive policy instead of only regulating the status quo. This in turn means there is a need for an own vision on digitisation, a well-informed opinion on which direction we want to take with digitisation, and a set of proactive choices to be made by the Dutch government to mitigate unacceptable non-European dependencies and add value on a national, European and global level.

Priorities in this respect for the Netherlands and Europe are:

- **Invest in technology development** for 6G, federated cloud, decentralised information & data infrastructures, trustworthy AI.
- **Stimulate the development of new business models** for decentralised information & data infrastructures, that ensure sovereignty.
- **Stimulate adoption of these technologies in key application areas** (e.g. Smart Health, Smart Mobility, Smart food & agriculture, Smart production, Smart security & cybersecurity, Smart Society) to ensure market-pull.
- **Set-up and strengthen international cooperation** in the aforementioned key technology development areas and application areas.

- **Stimulate the following opportunities**:
  - Smaller hardware (e.g. ICs), better batteries and antennas – that enable more pervasive computing, and decrease the need for centralised data infrastructures and data storage approaches.
  - Quantum technology.

Appendix A Visual on intra data space interoperability

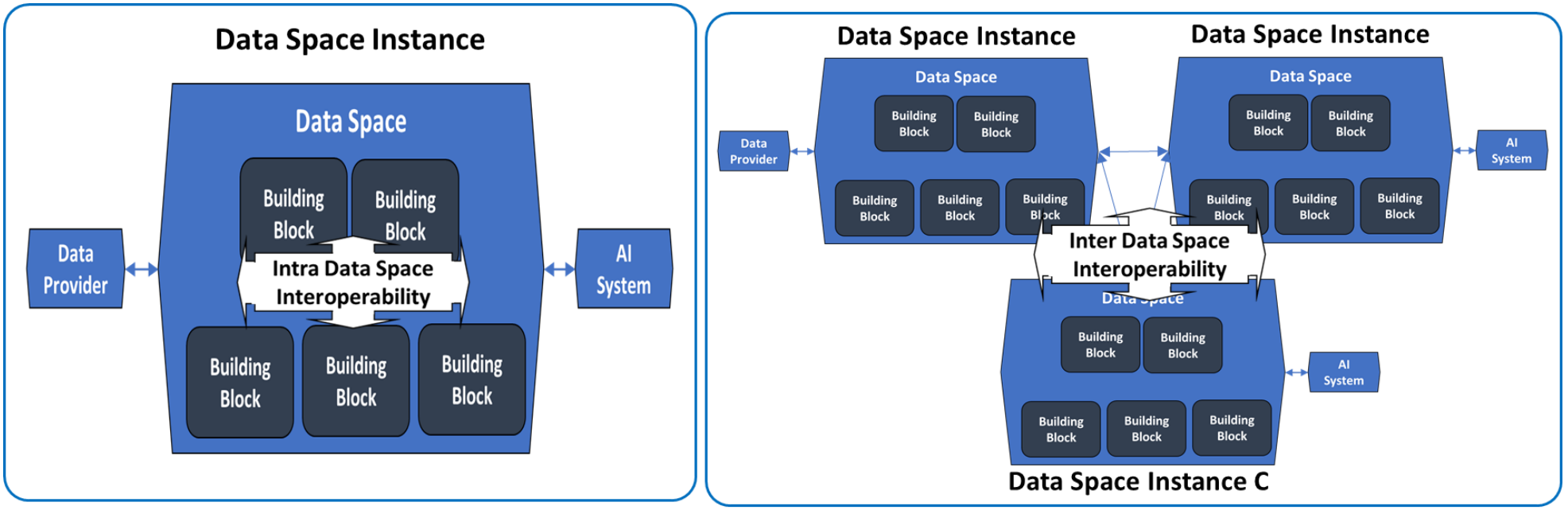


Figure 12. Intra data space interoperability (l) and inter data space interoperability (r) development lines.

Appendix B European reference architectures

European reference architectures

International Data Spaces (IDS).
IDS is currently gaining major international traction for realising an open network model approach for multi-lateral data sharing with infrastructural data sovereignty capabilities. The IDS reference architecture[244] is aimed at enabling the trusted sharing of sensitive data, whilst maintaining sovereignty. It can be considered an architectural elaboration of the NIST zero trust architecture [245]. It is based on peer-to-peer data sharing in a federated and open infrastructure for support services.

SSI (Self Sovereign Identity)
The term SSI is used for the development based on which a person or organization can create its own identity and manage this without the intervening of external administrative authorities. The aim is there that people can interact in the digital world with the same degree of freedom and trust as in the offline world. SSI is a way to digitally manage identities so that users are in control about their data [246]. A user has a personal safe in which he keeps various certificates, which he can demonstrate to organizations. The solution is privacy friendly in the sense that the user is in control about its own data.

SOLID (SOcial LInked Data)
SOLID, is a protocol specification that let people store their (linked-)data securely in decentralised data stores that are like secure personal web servers for your data. The specification enables (authenticated) applications to access this data if its owner has authorised this.

FEDeRATED and FENIX
The DTLF (Digital Transport and Logistics Forum) is the EC Directorate-General for Mobility and Transport (DG Move) initiative in the context of the EC policy to create a European Data Space for Supply and Logistics. Therefore, DTLF has initiated the Connecting Europe Facility (CEF) FEDeRATED Action [247] and the CEF FENIX Action[248]. Where FEDeRATED takes a top down approach driven by authorities and embedded in their national digitisation strategies, FENIX is driven by industry taking a bottom up approach by creating platform interoperability for a large number of use cases.
Although originating in the logistics and mobility sector, the FEDeRATED and FENIX data sharing concepts are sufficiently generic to be similarly applicable in other sectors as well.

GO FAIR
Arising from the need for management of and accountability for scientific data, the GO FAIR (Findability, Accessibility, Ínteroperability, Reusability) [249] principles and approach have been defined.
Although originating in the scientific domain, the GO FAIR data sharing concepts are sufficiently generic to be similarly applicable in other sectors as well.

Gaia-x
Aims to build a network of providers who develop and provide federated infrastructure services (IaaS/CaaS/PaaS) using precisely defined common standards, free software and documented operating processes , for more details see section 2.2.2.[250].

[244] IDSA (2019). “IDS-RAM 3.0”. 2019. URL: https://internationaldataspaces.org/ids-ram-3-0/
[245] National Institute for Standards and Technology (NIST), “Zero Trust Architecture”, NIST Special Publication 800-207, August 2020.
[246] I2P Foundation Wiki. “Self-Sovereign Identity’. URL: https://wiki.p2pfoundation.net/Self-Sovereign_Identity.
[247] FEDeRATED. “EU-project for digital cooperation”. URL: http://www.federatedplatforms.eu/.
[248] FENIX Network. “A European FEderated Network of Information eXchange in LogistiX - To support the transition to seamless data sharing”. URL: https://fenix-network.eu/.
[249] Go-Fair. “FAIR Prinicples”. URL: https://www.go-fair.org/fair-principles/.
[250] https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

Appendix C European regulation relevant for digital sovereignty

Why and how to regulate the digital?

Conceptualisations of how to regulate the digital are as old as Lessig's seminal laws of cyberspace[251], in which he argues that digitisation will have such a profound impact on society that it would require new forms of regulation to come to terms with it.[252] The challenges those new regulatory forms need to account for can be summarised as follows:

1) everything will become data-fied, but
2) the nature and logic of 'code' and data do not abide by rules that hold in the physical world (data is infinitely *copy-pastable*, for instance, and can be instantaneously shared across the globe); which means that
3) current legal regimes that aim at protecting people from harms inflicted by things, states and each other no longer suffice. The latter is further conditioned by
4) the lack of knowledge about the kinds of harm that can emerge from and through the digital domain, and how those will intertwine with our analogue-based lives and legal systems.

A case in point in that regard is that we still do not fully comprehend what data or big data truly *is* or how to define it,[253] as the technological developments that facilitate it evolve at a pace that hampers the longevity of any attempt to do so.

Contemporary endeavours to tame the 'digital wild west' amount to a vast and rather unstructured set or regulatory approaches[254] that originate from different jurisdictions and institutional levels - national, intranational, or international (the latter in the form of treaties or soft low strategies). The EU, for instance, opted for physical-world definitions of potential harms of digital technologies by connecting them to known frameworks and harm terminology. Data, in that regard, was divided into *personal* and *non-personal*, attaching to the former known harms (and a bit less to the latter), often in the form of privacy or other human rights-based harms and violations that have been projected onto digital technologies. Think here of the right to self-determination, which in Germany was translated into a right to *informational* self-determination.[255] Privacy in turn became synonymous with data protection, and early Data Protection regimes such as the DPD[256] were ramped up to create the GDPR which harmonised EU law on the protection of personal identifiable data. However, the technology neutrality of the GDPR, combined with an unstable socio-

[251] The Laws of Cyberspace (harvard.edu)
[252] A stance that up till this day is highly debated in legal scholarschip. See Brownsword, R. (2005). Code, control, and choice: why East is East and West is West. *Legal Studies*, *25*(1), 1-21.
[253] See Timan, T. (2018). Where and How to Find Data Definitions - Big Data Value (big-data-value.eu)
[254] Data governance and data policies at the European Commission | European Commission (europa.eu)
[255] Rouvroy, A., & Poullet, Y. (2009). The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy. In *Reinventing data protection?* (pp. 45-76). Springer, Dordrecht.
[256] Data Protection Directive, the predecessor of the GDPR

technical meaning and understanding of what personal data is,[257] has led to many instances of legal uncertainty or regulatory clashes that we are ongoing.[258] As a result, the GDPR's implementation presents a structural challenge for SMEs,[259] while at the same time appearing ineffective in making Big Tech giants comply with its provisions.[260] However, the jury is still out on the effectiveness of the data protection regulation, which some argue to be on the rise, since in July 2021 Luxembourg decided to hand Amazon a fine of €746 million for its improper handling of data breaches.[261] Beyond personal data protection, other forms of regulation and enforcement that the EU is pursuing to get a grip on the data economy in Europe are, for instance, fines and data-taxes, or stricter oversight.[262]

Where curbing Big Tech through the courts and financial institutions is one approach to regulating the effects of digitisation and the platform economy, there are many other strategies and initiatives aimed at shaping the digital age through, for instance, international cyber norms, the ongoing debate for an overarching cyber treaty and diplomacy. Noteworthy is the work of the UN Group of Governmental Experts (UNGGE) on voluntary international norms for the regulation of cyberspace (the co-called 'rules of the road') or the EU's sanctions regime against cyber-attacks, which was adopted in May 2019 [263] to deter and respond to malicious cyber activities on EU member states, third states and international organizations. In contrast to the data protection regime referred to above, these efforts do not protect individuals but provide the outlines of the playground, in which governments and international alliances level with each other in the digital domain. Accordingly, these frameworks address state responsibility, cyber attribution, capacity building, the protection of critical infrastructure, data breaches and theft, etc.

Other, more micro-level routes taken are those of techno-regulation and hard-coding of norms[264] through for instance Privacy Enhancing Technologies[265], as well as through establishing standards and certification bodies to help developers to self-regulate.[266]
On a national or regional level, digital regulation is usually preceded (or streamlined) by a publication of roadmaps and corresponding strategies.[267] The EU's ambition for Europe's digital transformation by 2030—the digital decade[268]— is also laid down in a recent strategy document. The latter lays emphasis on
1) increasing digital skills among the population and ICT specialists;

---

[257] Before the existence of mobile phones, for instance, location data was not personal, and now it is. Before the advent of web 2.0, an IP address wasn't either etc.
[258] See Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.
[259] STAR II Project (2019). D2.2 SME's experience with the GDPR. Results - star2project.eu (star-project-2.eu)
[260] Twitter hit with €450,000 GDPR fine nearly two years after disclosing data breach - The Verge
[261] With Amazon fine, Luxembourg emerges as Europe's unlikely privacy champion – POLITICO
[262] Digital Services Act: How the EU is going after Big Tech (cnbc.com)
[263] Council Regulation (EU) 2019/796 and Council Decision (CFSP) 2019/797
[264] Koops, B. J., & Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. *International Review of Law, Computers & Technology*, *28*(2), 159-171.
[265] Data protection in the era of big data for artificial intelligence_BDVA_FINAL.pdf
[266] Digital Services Act: How the EU is going after Big Tech (cnbc.com)
[267] National and International AI Strategies - Future of Life Institute; National Cybersecurity Strategies Repository (itu.int)
[268] Europe's Digital Decade: digital targets for 2030 | European Commission (europa.eu)

2) the digital transformation of businesses and adoption of innovative technologies;
3) creating secure and sustainable digital infrastructures (connectivity, semiconductors, data, and computing); and
4) digitalisation of public services. Moreover, there is a great geopolitical drive to capitalize on the benefits of digitalisation, which in the words of commissioner Breton is *"a global race in which the mastery of technologies is central"* .[269] The latter has become more than apparent for the key enabling technology of Artificial Intelligence (AI), the strive for which triggered enormous US investments, the European AI strategy, and the dramatic quote from the Russian president that the *"nation that leads in AI will be the ruler of the world"*.[270]

The EU's digital regulatory landscape

GDPR
It has been over 2 years since the introduction of the *GDPR*, the regulation aimed at harmonising how we treat personal data in Europe and sending out a message that leads the way worldwide. Indeed, many countries and states outside of Europe have since followed suit in proposing stronger protection on data trails we leave behind in digital and online environments.[271]

Free flow of data agenda, Public sector directive and the Database directive
In addition to the GDPR, the European Commission (EC) has proposed and instated a number of other regulations and initiatives that concern data. The *'free flow of data' agenda* is meant to lead the way in making non-personal data usable across the member states and industries,[272] the *Public Sector Information Directive* aims to open up public sector data to improve digital services or develop new ones,[273] and the *Database Directive* is aimed to set rules on the treatment of databases,[274] to name a few.

Regulations on cybersecurity and on data sharing (e.g. related to AI)
Steps have also been taken to harmonise cybersecurity approaches through the *NIS Directive*,[275] while on the other side, regulations for law enforcement on both the sharing of data across Member States and other nations (through the *e-Evidence Directive*)[276] and the specific ways in which law enforcement agencies (LEAs) are allowed to treat personal data (through the *Police Directive*)[277] have been put in place. On top of this already existing and complex set of data regulations, which sometimes overlap and sometimes exclude or preclude each other, the new Commission has put forward an ambitious agenda regarding

[269] The Geopolitics of Technology | LinkedIn
[270] Putin says the nation that leads in AI 'will be the ruler of the world' - The Verge
[271] The latter has become known as "the Brussels effect". See Bradford, Anu. *The Brussels effect: How the European Union rules the world*. Oxford University Press, USA, 2020.
[272] de Hert, P. , & Sajfert, J. Regulating Big Data in and out of the Data Protection Policy Field: European Data Protection Law Review Volume 5, Issue 3 (2019). pp. 338 - 351
DOI: https://doi.org/10.21552/edpl/2019/3/8
[273] Open data | Shaping Europe's digital future (europa.eu)
[274] Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform by Matthias Leistner :: SSRN
[275] NIS Directive | Shaping Europe's digital future (europa.eu)
[276] E-evidence - cross-border access to electronic evidence | European Commission (europa.eu)
[277] Police Directive | European Data Protection Supervisor (europa.eu)

Europe's further digitisation.[278] The latter places even more emphasis on getting data regulation right, especially in light of transitioning towards artificial intelligence (AI).[279] The main elements of this new digital agenda are the *Data Governance Act*,[280] which aims to harmonize the treatment and management of data, the *Digital Markets Act*,[281] aimed at regulating digital markets and building on, among others, the *ePrivacy Directive* which in short prohibits the use of cross-platform and cross-page tracking,[282] and finally, the *newly proposed regulation on AI*,[283] aiming to set rules and red tape for AI applications and systems in Europe.

These pillars on generic data and AI regulation have been and will be accompanied by specific challenges in an era of both digital acceleration and contested digital sovereignty, tied together by the question of how to keep some degree of control and steering possibilities for Europe.[284] One such challenge, for example, lies in how to effectively speed up the use of digital identities in Europe,[285] especially cross-border, or how to protect IP in (automatically) assembled datasets and algorithms.[286] Appendix D contains a (non-exhaustive) list of the most prominent digital regulations, which challenges or problem they address and what mitigating measures or innovation stimulation they promote: The list is comprised of both existing- and upcoming regulatory measures that help strengthen the Digital Single Market and contribute to a EU-specific stance on the interplay between digitisation and EU rights and values, thus in effect forming a set of norms that delineate where, how and over what the EU aims to develop forms of digital sovereignty.[287, 288]

AI as a new challenge for regulators

The EC is increasingly investing efforts in translating its data regulatory approach towards AI. Already before the ethical principle whitepaper was published, the EC and Member States individually have been engaged with the question of what and how to regulate when it comes to AI. Figure 13 provides an overview of regulatory steps taken so far:

[278] Europe's Digital Decade: digital targets for 2030 | European Commission (europa.eu)
[279] Adapted from Timan T., van Oirsouw C., Hoekstra M. (2021) The Role of Data Regulation in Shaping AI: An Overview of Challenges and Recommendations for SMEs. In: Curry E., Metzger A., Zillner S., Pazzaglia JC., García Robles A. (eds) The Elements of Big Data Value. Springer, Cham. https://doi.org/10.1007/978-3-030-68176-0_15
[280] Data Governance Act | Shaping Europe's digital future (europa.eu)
[281] The Digital Markets Act: ensuring fair and open digital markets | European Commission (europa.eu)
[282] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). COM/2017/010 final - 2017/03 (COD)
[283] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021PC0206&from=EN
[284] EU Digital Single Market | EU4Digital (eufordigital.eu)
[285] European Digital Identity | European Commission (europa.eu)
[286] Trends and Developments in Artificial Intelligence - Challenges to the Intellectual Property Rights Framework | Shaping Europe's digital future (europa.eu)
[287] See: Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. Philosophy & Technology, 33(3), 369-378.
[288] See: or Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: an analysis of statements and policies. Internet Policy Review.

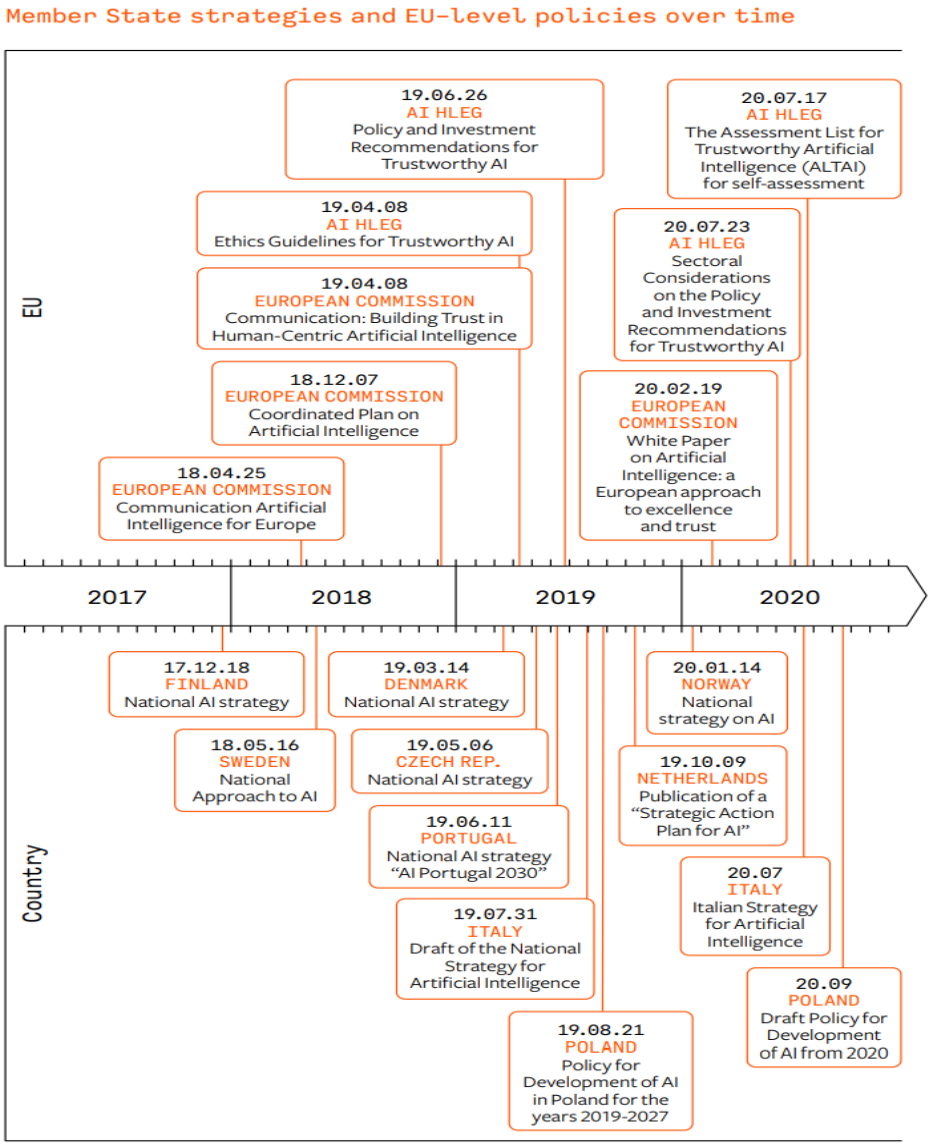


Figure 13: An overview of AI strategies and policies over time.

Both Member States and the EU's regulatory bodies (the EP and the EC most notably) have been active in shaping AI policies, strategies and guidelines[289] since 2017. Some countries have actually enacted law on AI, such as Denmark, which imposed a legal obligation on companies in the online space to release information about their data ethics policies.[290] In general, AI policies, strategies and regulation are closely monitored by the OECD.[291] From a regulatory perspective, some of the most pertinent debates concern the following:

- **AI personhood**. The EP's stance rejects this approach, arguing that AI should remain a tool in the hands of humans. Others see in legal personhood for AI an inroad to better regulate AI harms by way of offering a legal place of redress.[292]

[289] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/868284/Web_Version_AI_and_Public_Standards.PDF
[290] Denmark introduces mandatory legislation for AI and Data Ethics - 2021.AI
[291] The OECD Artificial Intelligence Policy Observatory - OECD.AI
[292] https://www.linkedin.com/posts/paul-de-hert-5600737_refusing-to-award-legal-personality-to-ai-activity-6740341186243907584-Mtip

- **IP and AI**. Here in particular the outcomes of Machine Learning and Neural Networks, and the often networked reality (system of systems) in which algorithms operate, make the question of allocating IP very complex.
- **Liability and human oversight**/control is pressing at the moment: at what point in AI-based decision-making processes does liability 'transfer' in a digital service, and does AI change qualitatively the nature of liability in decision-making or not?[293]
- How to curb **bias and unfair treatment** and novel forms of discrimination as a result of AI-based data processing, is also a pressing matter. Thus far, anti-discrimination law appears ill equipped (or 'used') in relation to data and AI, and data protection regulation is not at all equipped to deal with harms on a collective, structural and/or secondary scale.[294]

This list is however in stark contrast with the abstractly formulated AI strategies, especially those authored by individual Member States. In between the EU's digital agenda and the overarching layer of geo-political and Big Tech competing interests, for the time being there is limited room for Member States to actively shape solutions to these issues.

Data protection and anti-discrimination law

Where self-regulation through, for instance, standards or certification is industry- or sector-bound and therefor crosses boundaries more easily, regulation is often nation-bound, creating all sorts of interpretation and implementation challenges. Turning to AI and the role of regulation, currently there are only two 'regimes' or types of law in place that offer some form of protection to citizens against AI harms, *being data protection* and *anti-discrimination law*. On the consumer and business-to-business side, the current EU regimes of liability and product safety are of relevance, and will also impact the development of AI legal frameworks.

The role of data and AI regulation in digital sovereignty[295]

The data regulation landscape in Europe is complex, as is the data economy: translating the intrinsically global and cross-border nature of data flows coupled with an increase of automation in digital values chains with forms of digital sovereignty will be challenging. The proposed set of measures put forward by the current EC are ambitious, both regarding what should be prohibited or strongly regulated, as well as what should be promoted and how (for instance data cooperatives and data spaces such as Gaia-X)[296]. One of the reasons why data regulation is so complex, lies in the difficulty of defining and delineating it.[297] Data and its regulation impact companies, governments, organisations and citizen alike in a both generic and sectorial manner. Further, the GDPR is still seen by some as a strong regulatory force hampering data innovation. While its explicit data strong-arming is intended to curb the influence of large, mainly US-based tech giants,[298] there are many smaller,

[293] https://www.europarl.europa.eu/news/en/press-room/20201209IPR93411/artificial-intelligence-guidelines-for-military-and-non-military-use

[294] Some scholars argue the GDPR has all the elements in place to deal with AI-harms as well, while others see this as trying to squeeze larger systemic issues into data protection law, which perhaps regulates some potential harms of AI, but will miss out on many.

[295] See also Digital sovereignty for Europe (europa.eu)

[296] GAIA-X - Home (data-infrastructure.eu)

[297] Where and how to find data definitions - Portfolio Tjerk Timan

[298] https://www.euractiv.com/section/digital/interview/sam-francesca-bria-europe-cannot-rely-on-silicon-valley/

sectorial actors[299] that develop services in the EU or for European citizens and business that suffer from its legal force: start-ups and SMEs often lack the resources and skills to understand the vast and complicated landscape[300] created around data in Europe. This poses numerous problems for the regulator: on the one hand, we know that the reliance on self-regulation of platforms on regarding privacy or hate-speech, for instance, has been so far unsuccessful,[301] and that fines do not fundamentally affect or change big-data platform practices and business models.[302] Yet, all rules have to apply similarly to both large and foreign digital service providers, as to small EU-based start-ups. On the other hand, people expect EU and MS regulators to act strongly on disinformation, hate speech, privacy infringements and other harms caused by platforms that lie outside of EU jurisdictions. This ongoing puzzle for policymakers[303] has not been made easier with the recent focus on AI. Being placed next to, or on top of, ongoing debates on data regulation, the EC's ethical guidelines for the development of AI[304] have had quite the effect on an already enlivened debate on potential harms that stem from the (boundless) digital domain. Next to embodying Europe's vision for responsible AI that sets the EU apart from global competitors, the guidelines are also intended as a key component of increasing the EU's digital sovereignty by ensuring that European users have more participatory control.[305] There are now many attempts to translate some of the high-level principles to which AI should adhere into what this means for policymakers, regulation and digital service developers. While not all forms and sorts of AI pose threats or offer the (sometimes too far-fetching) promises attributed to it, concerns about the future and nature of work,[306] the way in which AI-based systems are reshaping our personal and professional behaviour,[307] to build-in or enforced bias in processes of automated decision-making and the role of AI in interacting with humans,[308] are at the forefront of such translation attempts.

Overall, the European position towards digital technologies and the regulation thereof creates a dilemma. There is potential for AI to be used in government, research and business to solve societal issues and realize economic growth. Yet, in many sectors innovation is a 'winner takes all' race, in which if actors obtain a dominant position in the market, they can easily defend it from challengers. This is especially true in markets where digital technologies and the data economy play an important role.[309] Early movers are in a strong position to shape the field and the rules, and to-date, successful early movers are overwhelmingly US- or China-based. Most digital innovations offering novel services stem from the US and most

[299] Spill-overs in data governance: the GDPR's right to data portability and EU sector-specific data access regimes - Big Data Value (big-data-value.eu)
[300] Deliverable D2.2 Report on Legal Issues — LeMO – Leveraging Big Data to Manage Transport Operations (lemo-h2020.eu)
[301] TikTok Rallies Facebook, Twitter to Regulate Harmful Content - Variety
[302] It can also be questioned whether we really want to rely on GAFAM to make up the rules of our online lives.
[303] See BDVE_Policy_Brief_read.pdf (big-data-value.eu)
[304] commission-white-paper-artificial-intelligence-feb2020_en.pdf (europa.eu)
[305] Brattberg, Erik, Venesa Rugova, and Raluca Csernatoni. *Europe and AI: Leading, Lagging Behind, Or Carving Its Own Way?*. Carnegie Endowment for International Peace., 2020.
[306] Cory Doctorow: Full Employment – Locus Online (locusmag.com)
[307] Companies are now writing reports tailored for AI readers – and it should worry us | Big data | The Guardian
[308] Turn that frown upside down - Emotional AI and Regulation (big-data-value.eu)
[309] CPB (2018). *Digitalisering R&D*. CPB Policy brief 2018/13.

hardware stems from Asia, more specifically China, leaving the EU in a weak position when it comes to shaping data and AI. From the perspective of Europe's economy and values system, if it fails to develop homegrown AI-supported businesses, a situation will continue where almost no tech giants are based here and Europe risks becoming a 'rule-taker'.[310] This is a race in which Europe does not want to be left behind. It is also with the latter in mind that critique on the draft AI act has been formulated. Some see its release as early and premature, since efforts towards developing AI "made in Europe" are still at a preliminary stage. While regulation is much necessary, it should facilitate a dialogue between society's interests and the needs/ results of innovation.

[310] Çharlemagne, 'Waiting for Goodot', *The Economist*, October 13 2018.

Appendix D European legislation with a digital scope

(D= directive, R = regulation, N=non-legislative. Proposals are marked with an *, expected proposals are marked with a ?)

Legislation	Year	Type	Policy area	Topics	Aim and AI/digital relevance
Database directive	1996 *(2022?)*	D	Digital	Intellectual property rights, copyright	To provide a legal basis for the treatment of databases under copyright law. The directive is currently under review for revision.
Directive on intelligent transport systems (ITS)	2010 *(2022?)*	D	Transport, industry	Data, Interoperability	Legal framework for the interface between road transport and other transport modes. The directive has been reviewed for revision.
Payment Services Directive (PSD2)	2015	D	Financial technology	Data, Interoperability	To provide the legal foundation for the further development of a better integrated internal market for electronic payments within the EU.
European Pillar of Social Rights	2016	N	Skills, employment, education, health	Labour market, working conditions, social protection and inclusion	Principles, not legislative but a driver for legislative change. Relevant for gender, and race equality strategies: Tackling discrimination through AI, combatting (gender) stereotypes
Directive on security of network and information systems (NIS2)	2016 2020*	D	Digital, energy, transport, financial technology, health	Cybersecurity	To ensure the preparedness of member states for security incidents, strategic cooperation and create a culture of security across sectors that rely on ICT.
General Data Protection Regulation (GDPR)	2016	R	Digital	Data	To lay down rules for the protection of natural persons in the use of their personal data.
Police directive	2016	D	Digital, defence	Data, Justice	Legal framework for personal data use in law-enforcement activities ('lex specialis' to the GDPR)
ePrivacy Regulation (ePR)	2002 (D) 2017* (R)	D	Digital	Privacy, Data	Regulation of privacy-related topics regarding electronic

					communications ('lex specialis' to the GDPR)
Free flow of non-personal data	2018	R	Digital	Data	Removing obstacles to the free movement of non-personal data between different EU countries and IT systems in Europe.
e-Evidence directive	2018*	D	Digital, defence	Data	to simplify law enforcement authorities' ability to access data held by digital service providers in another national jurisdiction
Open Data Directive	2019	D	e-Government, Digital	Data	Provides common rules for a European market for government-held data.
Data Governance Act	2020*	R/ D	Digital	Data	To facilitate trustworthy data sharing across sectors and member states.
Markets in Crypto-assets (MiCA)	2020*	R	Financial technology	Digital assets	To harmonise the European framework for the issuance and trading of various types of crypto tokens as part of Europe’s Digital Finance Strategy
Digital Markets Act	2020*	R/ D	Digital	Competition	To ensure a higher degree of competition in European digital markets, attribute responsibilities to *Gatekeepers*
Digital Services Act	2020*	R/ D	Digital	Contents, transparency, advertising, disinformation	To modernise and create an EU-wide uniform framework on the handling of illegal or potentially harmful content online, the liability of online intermediaries for third party content, the protection of users' fundamental rights online and bridging the information asymmetries between the online intermediaries and their users. *(complementary to the e-Commerce directive)*
Artificial Intelligence Act	2021*	R	Digital	AI	- Risk-based legal framework for the regulation of AI - Regulatory sandboxing for the development and use of AI

Data act	2021*	R/ D	Digital	Data	To set the right conditions for better control and conditions for data sharing for citizens and businesses.
Digital levy	2021*	D	e-government, financial technology	Taxation, Competition	To introduce a digital tax to address the issue of fair taxation of the digital economy.
New European digital identity framework	2022*	N	Digital, e-government	Data, Privacy, Identity	- To make it easier to do tasks and access services online across Europe - To ensure people have greater control and peace of mind over what data they share and how it is used
Legislative proposal to improve the working conditions of people providing services through platforms	*(2022?)*	R/ D	Digital, employment, industry, e-government	Labour market, working conditions, social protection and inclusion	To ensure fair working conditions and adequate social protection for labourers through digital platforms. *Note that many of these platforms use AI in their services (e.g. automatically matching supply and demand)*

Appendix E Business models for digital value propositions

Business Model Canvas

Several tools have been proposed in literature to support the design of (digital) business models. Prominently used and popularised in both academia and practice, Osterwalder & Pigneur (2010) propose the Business Model Canvas (BMC). The BMC represents a graphical template encompassing nine building blocks that can be used to describe the business or value logic of a business model design as well as the core mechanisms that support or underlie the business model design (see Figure 14). These building blocks refer to *key partners, key activities, key resources, value propositions, customer relationships*, *customer segments*, *channels*, *cost structure* and *revenue streams*, addressing the various concerns related to business modelling. One can see that the BMC targets the design of business models for a single organization (e.g. *firm-centric*), focusing predominantly on how internal and external resources (such as the resources of partners) can be leveraged to support the business logic and to create value for various customer segments.

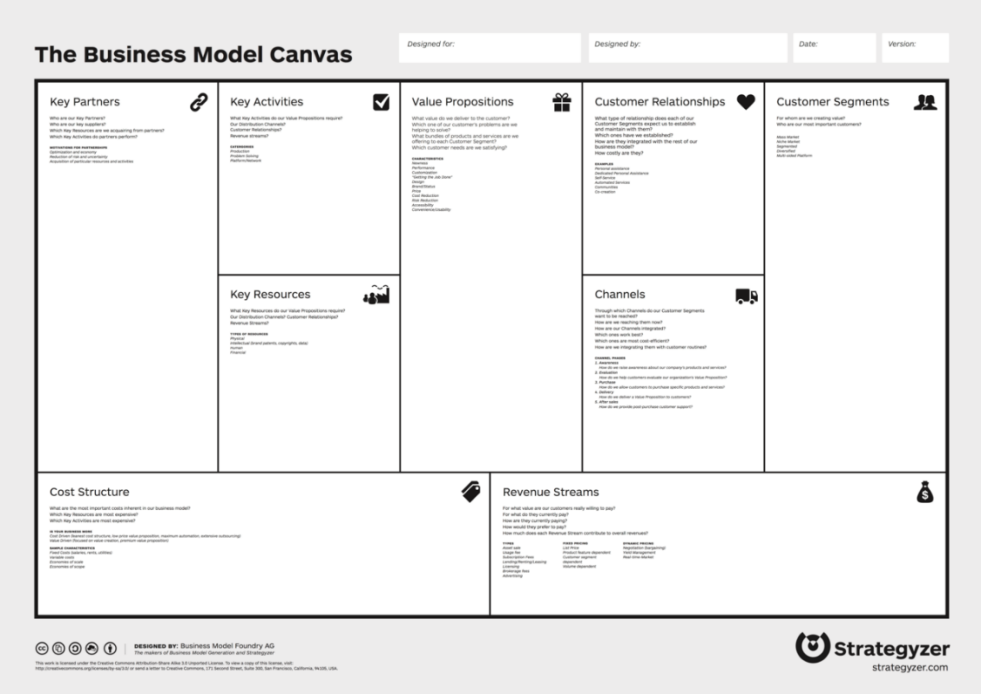


Figure 14. Business Model Canvas Template

Platform business model canvases

Building upon the application logic and general structure offered by the BMC supporting the representation and design of business models, several derivate tools have been proposed targeting the design of platform-based business models. The Platform Business Canvas (PBMC) (Eisape, 2019), which is depicted in Figure 15, offers a network-oriented view on how stakeholders collaborate on and interact through platforms. One can see that each of the generic stakeholder roles represents adopts a structure analogously to the original BMC, extended through

concerns that are specific to platform business models (such as the pains and gains generated through participation or individual concerns such as the governance of the platform). For the stakeholder roles, a distinction is made between stakeholder roles that are external to the platform (such as customers or providers) and stakeholder roles that are internal (such as partners and the owner or orchestrator of the platform). Accordingly, through use of the PBMC, the business model structure pertaining to any platform business setting can be captured and described.

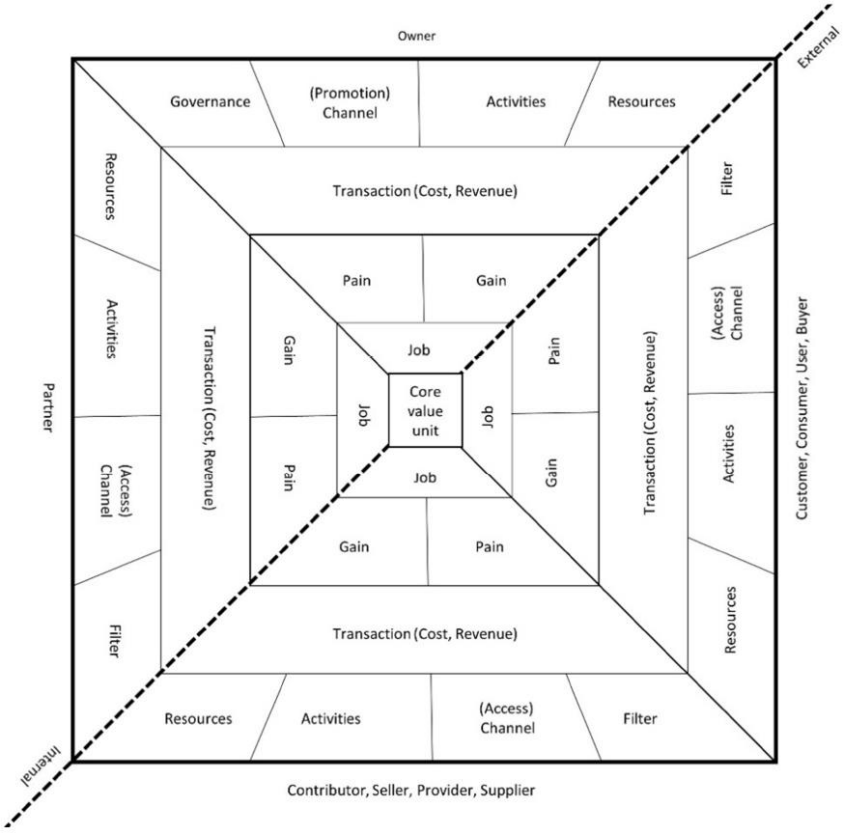


Figure 15. Template for Platform Business Model Canvas (PBMC)

STOF

Focusing on business models towards servitization or service provisioning, Bouwman et al. (2008) propose the STOF model towards the design of business models. The STOF model consists of four interlinked domains (namely Service, Technology, Organization and Finance) that jointly explain how value can be created for customers or different service providers (see Figure 16). The starting point for any business model is the *Service domain*, addressing the value proposition central to a business model for a specific target group or customer segment, as well detailing the service offering through which this value is proposed. Logically, novel service offerings pose requirements with regards to the technical architecture needed to support the delivery and operation of such services. Such requirements are addressed for the *Technology domain*, clarifying and explicating the technical or software components needed to provide the proposed service offering. Next, the *Organization domain* delineates the organizational resources and capabilities needed to support the business model design. Whilst for STOF services are typically offered by a single organization, it is expected that this organization collaborates with external organizations and thus is able to build on both internal

and external resources, relationships and capabilities and to integrate such competencies towards the provisioning of the service. Lastly, the *Finance* domain details the revenue model underlying the business model design, explicating how business model investments are financed, what pricing schemes are adopted and explaining the financial viability of the business model design.

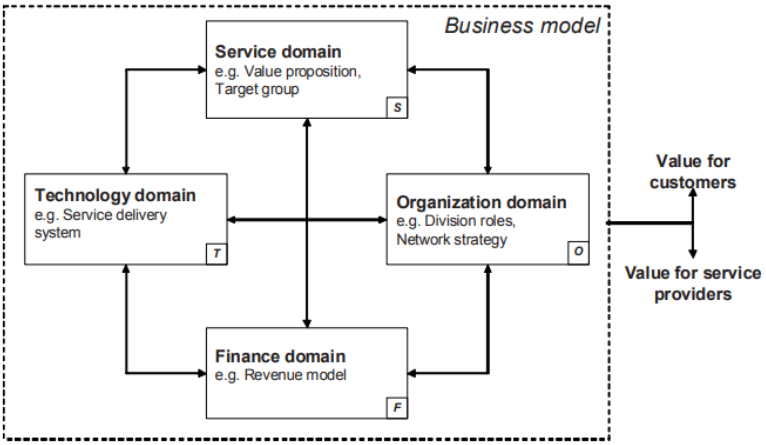


Figure 16. STOF Model

e3-value modelling

Originating from e-business research, Gordijn & Akkermans (2001) propose the e3-value modelling approach, which builds upon its own ontological basis and adopts its own modelling notation (illustrated in Figure 17). In contrast to the BMC and STOF, e3-value models generally capture the design of business networks or ecosystems that focus on the provisioning of a service to the target or customer segment (Gordijn, 2004). This means that users are able to represent and describe bilateral relationships and exchanges that exist between business network stakeholders. Business models designed through e3-value modelling contain three viewpoints, namely the *global viewpoint* (detailing the actors that participate for the business network as well how objects or value is exchanged between these actors), the *detailed actor view* (describing how actors may consist of constellations of sub-actors) and the *value activity viewpoint* (detailing what activity each elementary actor conducts to create or add value). Accordingly, the set of viewpoints can be used to detail business model concerns such as the business logic, core mechanisms and resources needed.

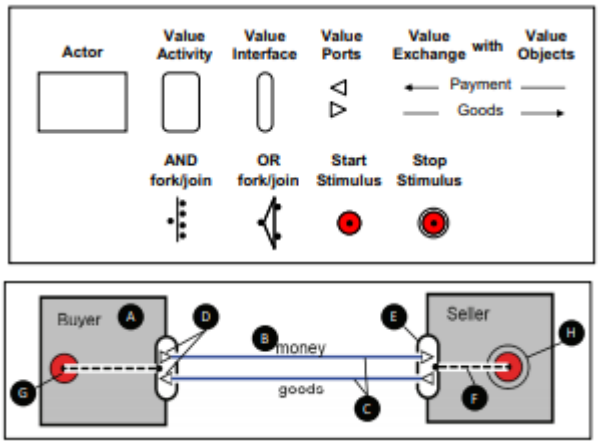


Figure 17. e3-value modelling notation and structure

Service-Dominant Business Model Radar

Building upon the principles of service-dominant logic, Lüftenegger (2014) and Turetken & Grefen (2017) propose the Service-Dominant Business Model Radar (SDBM/R) for the representation of service-driven, collaborative business models. The template of the SDBM/R is illustrated in Figure 18. One can see that the SDBM/R is divided into 'pie slices' (representing the actors in the business network), which intersect at the center, representing the *co-created value in use* (e.g. the value that collaboratively is established by the network and offered to the target customer). Note that each business model design always consists of *a customer*, *the focal organization* and at least one *additional business network actor*. Each of the pie slices consequently is divided by into three rings. The inner ring describes the *actor value proposition*, detailing the value that each individual actor in the business network contributes towards the co-created value in use. The middle ring describes the *actor co-production activity*, delineating the resources deployed and activities conducted to generate the proposed value. Lastly, the outer ring describes the actor specific costs and benefits that are generated through participation in the business model design.

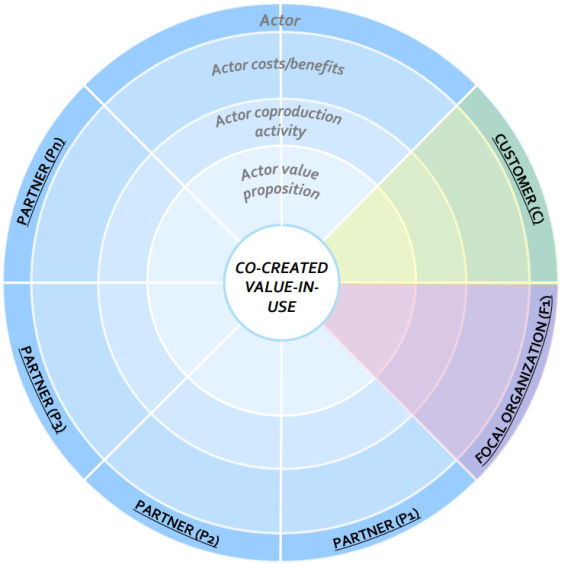


Figure 18. Service-dominant Business Model Radar (SDBM/R)

DAMIAN

Focusing on the provisioning of digital services, Berkers et al. (2014) propose the DAMIAN method. DAMIAN facilitates the systematic analysis and description of how service delivery is orchestrated for the value web, highlighting the specific activities that should be conducted to establish and deliver a proposed service to the target group or customer and indicating which organizations are involved to do so. In addition, it enables users to clarify the rules and regulations that may impact how organizations interact within the value web. Accordingly, DAMIAN addresses the various concerns relevant for designing business models. DAMIAN does so partly by incorporating a service delivery canvas template that facilitates users to model what organizations are involved for establishing the service (offerings), what architecture is needed to distribute the service and how customers can access or consume the proposed service (see Figure 19).

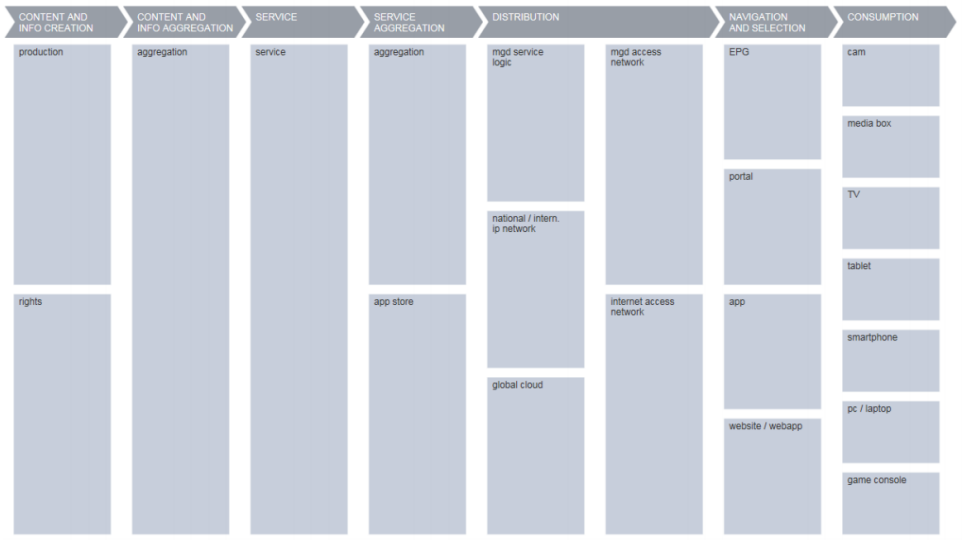


Figure 19. Service Delivery Canvas (as included for DAMIAN)

Appendix F Common business roles for data-driven or digital business models

One avenue for future development of the knowledge base on collaborative business models for digital-enabled services is to look at *business model typologies* that are catered to digital innovation or digital business. With regards to the topic, some preliminary research work has already been conducted. For example, Cambridge research[311] has investigated based on a set of both established large companies as well as start-ups in domains such as retail, logistics, telecom, insurance and finance, how big data is generated and used to service business purposes. In such domains, (the generation and use of) big data is increasingly becoming vital to sustain and strengthen business competitiveness. Their research has identified generic categories with regards to the purpose of data (e.g., to increase expansion of business or to shorten supply chains), the sources of data (e.g., free, customer-provided or acquired), processing of data (visualization, distribution, or visualization) and what potential revenue models can be pursued based on data. In doing so, they have generated a set of common business roles that can be expressed for data-driven or digital business models, as illustrated in Figure 20. Here, five types of generic stakeholder roles that may feature in data-driven business models are identified, namely:

- *Data publishers,* addressing the dissemination and publication of raw data to be used elsewhere.
- *Data extractors or transformers*, responsible for extracting and transforming raw data into data elements that can be used as input for internal and external processes or decision making.
- *Data analyzers*, focusing on visualization and analysis of data to support decision making.
- *User experience providers*, building upon data to provide service-based solutions or platforms to end-users.
- *Support service providers*, offering consulting-based services in the context of data.

These generic roles can be compared to roles corresponding to big-data business models, for which three common roles are identified, namely *data users* (using data to drive internal purposes), *data suppliers* (market big data as means of revenue) and *data facilitators* (supplying data users with infrastructure solutions and big-data driven services) . [312]

[311] Brownlow, J., Zaki, M., Neely, A., & Urmetzer, F. (2015). Data and Analytics – Data-Driven Business Models: A Blueprint for Innovation. *Cambridge Service Alliance*, 7, 1-17.

[312] Wiener, M., Saunders, C., & Marabelli, M. (2020). Big-data business models: A critical literature review and multiperspective research framework. *Journal of Information Technology*, *35*(1), 66-91.

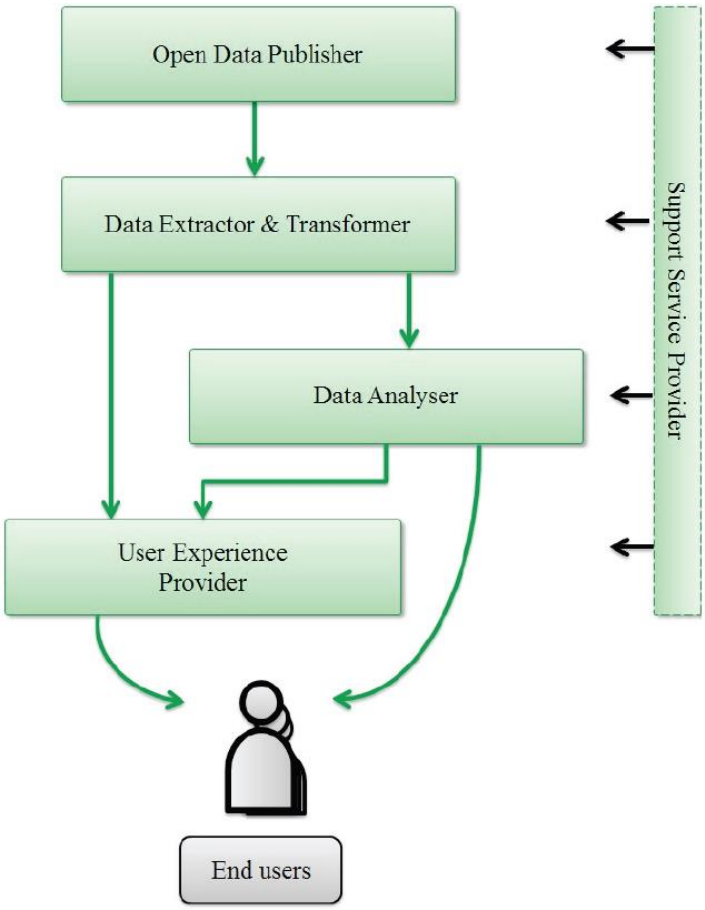


Figure 20. Generic stakeholder roles for data-driven business models

In the context of distributed ledger-based business models (i.e., business models for which transactions are recorded without a centralised database), we see that complementary roles are introduced[313]. Cryptocurrency business models (considered as an example of such DLT business models) may feature roles such as the *data infrastructure provider* (offering the general infrastructure distributed ledger database), a *development facilitator (*offering software platforms for the development of blockchain-based applications, an *integration enabler* (offering support services to foster the integration of applications), *application providers (*offering concrete, holistic applications) and *supplementary service providers (*aiding or consulting users on establishing protocols and standards).

What we can conclude from these generic stakeholder roles is that effectively any new digital business model is characterised by significant interdependencies and interconnections between stakeholders. For example, data that is generated by extractors or available at publishers serves as the basis for analysts or service providers to create value through digital services or solutions in business models. Here, even interrelationships can exist between different business models, creating a network of interactions between digital stakeholders.

313 Lindman, J., Kinnari, T., & Rossi, M. (2015). Business roles in the emerging open-data ecosystem. *IEEE Software*, *33*(5), 54-59.
Rückeshäuser, N. (2017). Typology of distributed ledger based business models.

In addition to understanding the interrelationships between stakeholder roles, these references business models and generic stakeholder roles can, on a macro-level, also help us to identify where potential challenges lie for European initiatives in terms of digital sovereignty.

Appendix G The impact of the Big Tech scenario

As long as the aforementioned key issues are not solved the Netherlands and Europe remain in the Big Tech dominance scenario. This means a large dependency of the Netherlands and Europe on foreign digital technology, which has a negative impact on four levels: Economic, Innovation, Societal and Geopolitical. This box describes this impact on European level (including the Netherlands).

Economic impact
Europe is a major player in the world economy. The continent is the second largest market in the world after the United States, with more than 746 million people and 22% of the world's GDP.[314] Europe is also home to some of the world's most important industrial firms, large automotive companies, and leading telecom firms. Besides that, there are large research facilities and research communities within the EU. Over the last 20 years, the EU has taken the leadership position in the scientific literature, ahead of the US.[315] While the EU has a strong presence of various industries and research communities, the digital economy is highly concentrated in the US and China.[316]

When the COVID-19 pandemic hit the world, the dependence on the digital technologies, cloud, and all things digital, became even more apparent. The competitiveness of the EU digital space has become questioned as many rely on a limited number the digital platforms and technologies of non-European origin. In order to turn this situation and to strengthen EU's digital sovereignty, a culture of innovation where digital companies and start-ups can excel is of importance. [317] However, when new potential competitors arise, Big Tech companies have the tendency to acquire those (European) start-ups that challenge them in their market.[318] The advantage is that these acquisitions speed up the spread of innovations. The disadvantage is that this means a barrier to entry, lack of competition which could adversely affect the setting of fair prices and the quality of products, as well as innovation (the later will be discussed in the next section).[319] It also means a growing number of economic sectors that are becoming increasingly and quickly dependent on foreign high tech companies and dominant platforms.[320] Potentially, it also means that the non-EU companies enter critical infrastructure markets such as data centres.[321] Furthermore, the dominant position held by the main digital platforms has favoured the implementation of complex tax optimisation and tax avoidance frameworks.[322]

Besides that Big Tech don't reinvest their profits where they were made, but ship them to their own enclaves[323]; The electronics store where people bought their

---

[314] https://www.oodrive.com/blog/regulation/digital-sovereignty-and-economic-growth/
[315] Melissa Flagg, Autumn Toney, and Paul Harris, "Research Security, Collaboration, and the Changing Map of Global R&D" (Center for Security and Emerging Technology, June 2021). https://doi.org/10.51593/20210004.
[316] https://ecipe.org/wp-content/uploads/2021/03/ECI_21_PolicyBrief_03_2021_LY03-1.pdf
[317] DGAP 2021. Europe's capacity to act in the Global Tech Race. P. 23
[318] Big tech dominance (2) : a barrier to technological innovation ? - Fondapol
[319]https://www.lecese.fr/sites/default/files/travaux_multilingue/2019_07_souverainete_europeenne_numerique_GB_reduit.pdf#page8
[320]https://www.lecese.fr/sites/default/files/travaux_multilingue/2019_07_souverainete_europeenne_numerique_GB_reduit.pdf
[321]
https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf
[322] Ibid
[323] https://www.trouw.nl/politiek/u-wordt-digitaal-gekoloniseerd~b6b02f4f/

razor in the 1990s employed local people, and probably sponsored the local sports team as well. In the meantime that retailer has been outcompeted by an online store that can sell products below cost thanks to billion-dollar investors who prioritize growth over short-term profit and rely on data profiles that can offer cheap razors precisely to people who are looking for one. Such an online store does not invest in local communities, on the contrary.

Innovation impact

The dependency of Europe on foreign digital technology also has an impact on innovation. When it comes to data, that is the main raw material of the digital economy, 92% of the western world's data is stored in the US. [324] Potentially, this might mean that the data access and data sharing are hampered. Therefore hindering or restricting innovative potential inherent in data, because it is a crucial input to artificial intelligence, to many online services, production processes and logistics.[325]

This impact is worrying, especially since the innovation intensity in Europe is lower dan their foreign rivals. [326] Even though Europe has the largest investment in public R&D, its private investment in R&D in general (19%) is lagging behind in comparison with China (24%) and the United States (28%).[327] Europe (12%) has the lowest percentage of R&D investments in technology compared to the US (63%) and China (25%).[328] European firms on the list of the world's 500-largest tech companies invested a total of 27 billion euro in tech research and development in 2018.[329] That was half of the investments of the Chinese firms on the list, which invested 50 billion euro; and 1/5 of the amount invested by US firms on the list, which invested 134 billion euro.[330] (Europe and the US have similar GDPs, while China's is about 70% of that size).

The current dominance of Big Tech also has an impact on the type of innovation that takes place within this domain. Innovation can take place in many forms, from an open innovation model (e.g. focusing on the development of open-source software, where knowledge is freely available and cannot be claimed), to closed innovation (where companies work with 'trade secrets' and protect their knowledge from outsiders). Another model of innovation is the mixed innovation model of open and closed innovation, where companies claim their knowledge in patents and literature, which enables that this knowledge can be used by others under certain conditions.[331] Big Tech companies such as Apple apply a closed innovation model to develop for instance innovative cyber security and privacy solutions. This may hamper open innovation and sharing of knowledge, and the potential to create disruptive innovations.[332]

Societal impact

The increasing dependence on the digital infrastructure and digital technologies of a limited number of dominant foreign market players, also has a societal impact, which can be summarised as follows: Each day reveals new harms caused by Big

[324] https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/
[325]https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf
[326] Ibid
[327] mgi-reviving-european-innovation-vf.pdf (mckinsey.com)
[328] https://www.oliverwyman.com/our-expertise/insights/2020/sep/european-digital-sovereignty.html
[329] Ibid
[330] European Commission: "The 2019 EU Industrial R&D Investment Scoreboard".
[331] TNO (2019). Onderzoek naar het versterken van de innovatieketen op het terrein van cyber security. R10769. P. 36
[332] TNO (2019). Onderzoek naar het versterken van de innovatieketen op het terrein van cyber security. R10769. P. 36

Tech to public values[333]; Hate speech goes viral, advertising companies oversee and own massive information ecosystems, and private firms sell intrusion systems online, that have similar capacities to intelligence agencies.

The Social media platforms increasingly determine the rules of the game of our democracy, due to their lack of measures to counter dis-and misinformation, fake news and political influence (e.g. during elections) on their platforms.[334]

A strong dependency on non-European high tech giants brings control of other countries, which have different rules regarding espionage, privacy and issuance of data. This contributes to various issues such as algorithmic in-transparency, privacy breaches, illegal data transfer etc.[335]

Big Tech companies also copy practices of colonialism[336]; They enter our society to extract profit from it. Google Maps is the standard example, but also Pokémon Go, a worldwide hype in 2016. It collected data about the movements of players, who searched the streets while looking for virtual Pokémons, and sold it for advertising purposes. But it also steered players in the desired direction, placing Pokémons near companies that paid for such ways of attracting potential customers.

Geopolitical impact

Last but not least there is also a geopolitical impact. Managing geopolitical risks was before just about anticipating and preparing for physical disruption in volatile regions in the world and understanding how this may impact the business environment.[337] Not an easy task, but one in which risks were visible, easy to define and played out on a global stage.[338] These days geopolitics is increasingly being played out via an undefined technology race (between the US and China, with Europe in the middle) as states become aware that technology give them a strategic advantage.[339] States are no longer seeking for military advancement, but trade and cyber security advantage.[340]

Digital technologies became an important source of this geopolitical tension and for the battle for global leadership and growing geopolitical tensions between the US and China (often called the tech cold war).[341] The battle mainly concerns the leadership in the field of 5G, computer chip technology, and Artificial Intelligence (AI). Both the US and China play in this regard the sovereignty card. An example is the American ban of Huawei as a supplier of American telecom infrastructure.[342] Or the popular Chinese apps – such as TikTok and WeChat that are banned by the US for “national security, foreign policy and economic reasons”.[343] Experts indicate that this (digital) technology war is only in its infancy, meaning that an even stronger geopolitical impact is expected.[344]

---

[333] https://www.ft.com/content/9adb3a15-d610-4bd6-bae0-a87dc4f315c6
[334] https://userfiles.mailswitch.nl/files/3443-acde5625f3ee1664315ae1ef6132a594.pdf
[335] Ibid
[336] https://www.trouw.nl/politiek/u-wordt-digitaal-gekoloniseerd~b6b02f4f/
[337] https://csuite.raconteur.net/business-risk/the-impact-of-technology-on-geopolitical-risk/
[338] Ibid
[339]Ibid
[340]Ibid
[341] 3 https://usinnovation.org/news/whos-winning-tech-cold-war-china-vs-us-scoreboard.
[342]https://www.uu.nl/sites/default/files/Moerel%2C%20Timmers%20%282.0%29%20-%20Preadvies%20Staatsrechtconferentie%202020.pdf
[343] https://www.uu.nl/sites/default/files/Moerel%2C%20Timmers%20%282.0%29%20-%20Preadvies%20Staatsrechtconferentie%202020.pdf
[344] Ibid

Appendix H List of external experts consulted

List of experts consulted during an interview	
Name	**Function**
Arie van Bellen	Director ECP Platform voor de Informatie Samenleving
Jos de Groot	Director Digital Economy Ministry of Economic Affairs & Climate Policy
Boris Otto	Professor for Industrial Information Management at TU Dortmund University and Executive Director at Fraunhofer ISST
Paul Timmers	Visiting Professor University Wien, KU Leuven and Research Associate University of Oxford
Sander van der Waal	Research Director Waag