Report

Towards a sovereign digital future – the Netherlands in Europe

Authors

Claire Stolwijk, Matthijs Punter, Paul Timmers,
Julian Rabbie, David Regeczi, Simon Dalmolen

Februari 2024

TNO Vector
Centre for Societal Innovation and Strategy

Contents

Project number
060.55452/01.01

Abstract

Digital technology is changing people's lives. The EU's digital strategy aims to make this transformation work for people and businesses, while helping to achieve a climate-neutral Europe by 2050.[1] The European Commission is determined to make this Europe's "Digital Decade". Digital technologies are changing peoples' lives - from the way we communicate to how we live and work.

Digitalization has the potential to provide solutions for many of the challenges Europe and Europeans are facing and offers various opportunities such as[2]: Creating jobs, advancing education, boosting competitiveness and innovation, fighting climate change and enabling a green transition. To make our societies and economies fit for the digital age, the EU is committed to creating a safe digital space for citizens and businesses in a way that is inclusive and accessible for all.

This means enabling a digital transformation that safeguards EU values and protects citizens' fundamental rights and security, while also enhancing the digital sovereignty of Europe and the Netherlands.[3, 4] This is needed because:

- Most of data from the West is hosted in the US.[5]
- The core of the digital infrastructure is provided by non-European suppliers (e.g. for routers, switches, encryptors and servers).[6]
- The seven largest tech firms in the world, by market capitalization, are all American.[7]

Digital sovereignty is on the political agenda. It can be defined as: *"control over the design and use of (business) critical digital systems, algorithms and the data generated and processed with them"*.[8]

Digital sovereignty means having the digital capabilities and capacities to produce, deliver and use digital goods, services, and infrastructures and having control over these in order to safeguard sovereignty. In the digital domain, Europe is primarily focusing on regulatory power, through for instance the General Data Protection Regulation (GDPR), the Data Governance Act, and the Digital Markets Act (DMA) and Digital Services Act (DSA), the Network and Information Security Directive (NIS) and the AI Act. Europe claims moral and legal authority, in which, for example, privacy is regarded as an individual fundamental right that needs to be collectively safeguarded and not as something that can be left to arrangements between the individual consumer and service provider through conditions and settings.[9] The President of the European Commission Ursula von der Leyen said about this; *"you must not only regulate, but also have the technology to anchor your own values"*.[10] This involves a balancing act when achieving a certain degree of autonomy and self-reliance without pursuing protectionist policies, a characteristic of open strategic autonomy to which the EU and the Netherlands subscribe.

1 A Europe fit of the Digital Age: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en
2 A Digital Future for Europe: https://www.consilium.europa.eu/en/policies/a-digital-future-for-europe/
3 Ibid
4 Who owns data and who controls it? | World Economic Forum (weforum.org)
5 Digital sovereignty for Europe, EPRS Ideas Paper. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf
6 Based on expert input.
7 Europe has fallen behind America and the gap is growing (June 2023): https://www.ft.com/content/80ace07f-3acb-40cb-9960-8bb4a44fd8d9
8 Based on Reflecties over digitale soevereiniteit https://www.uu.nl/sites/default/files/Moerel%2C%20Timmers%20%282.0%29%20-%20Preadvies%20Staatsrechtconferentie%202020.pdf
9 Ibid
10 Ibid

In this report we provide an overview of the level of digital sovereignty for Europe and the Netherlands based on the various digital technology layers of a stack model. Per technology layer a distinction is made between R&D, commercialization and policy and regulation to indicate how dependent Europe and the Netherlands are on a limited number of non-European players. In addition, this report provides key perspectives on digital sovereignty, namely the socio-economic, company/ organization, and cybersecurity perspectives. Based on this we apply scenarios to indicate:

1. The current situation,
2. The situation if no additional policy measures are taken and
3. The ambition.

In order to realize the ambition three types of measures are provided:

1. Current measures,
2. Additional measures and
3. Ambitious measures.

1. Introduction

Europe's digital transformation is one of the key priorities of the European Commission as digital technologies are critical for societal and economic progress. The overall strategy is to improve digital infrastructure and connectivity across Europe to boost competitiveness and the energy and green transitions. However, Europe is limited in its powers and means to decide on its own future in this digital transformation. Europe has limited digital sovereignty. The reasons are the power of foreign big tech giants like the US (Google, Facebook or Amazon, Apple, NVIDIA, Microsoft) and China (Baidu, Alibaba, Xiaomi or TikTok), geopolitical tensions, and global challenges that surpass a single country such as climate change, pandemic, and cyber-crime. Therefore, the European commission and the Netherlands see Digital Open Strategic Autonomy (DOSA) as an important priority. According to the "Kamerbrief of October 17 2023" about the Agenda Digital Open Strategic Autonomy DOSA means *"being open to the outside world, and protective in the digital domain when needed"*.[11] In another "Kamerbrief of November 8 2022" Open Strategic Autonomy is defined as *the ability as a global player, in collaboration with international partners, to safeguard own public interests on the basis of own insights and choices and to be resilient in a connected world.*[12]

To become more strategic autonomous in the digital domain one needs digital sovereignty. We define digital sovereignty as ***"control over the design and use of (business) critical digital systems, algorithms and the data generated and processed with them".***[13] Digital sovereignty means having the digital capabilities and capacities to produce, deliver and use digital goods, services, and infrastructures and having control over these in order to safeguard sovereignty.

Digital sovereignty can be identified with DOSA. Governments *"are pushing to reform the digital jungle"* to become more digital sovereign. They are mainly doing that based on regulation, but they also have various other policy instruments in place (e.g. awareness creation, stimulating innovation etc.). Today's conversation about digital sovereignty started with the need for more respect of the privacy of persons (e.g. this provided the GDPR) and businesses to maintain control over their digital infrastructure, data and technology. According to the International Data Corporation, it was predicted before that by 2024, 65% of major enterprises will mandate data sovereignty controls – or the storing of data within national boundaries – from their cloud service providers, so that businesses can adhere to the data protection requirements set out by host countries.[14] Governments are now asking if they can have full trust in the technology they are using with the increasing interconnectedness of digital systems.[15] Without digital sovereignty, there is the potential that for instance cyber-attacks can disrupt critical infrastructure, undermine national security, or even put citizen safety at risk.[16] Central to having control over one's digital destiny is knowing where the technology comes from and what your software is exposed to – formulated differently, having full visibility.

When digital sovereignty is expressed in a data and a technology pillar[17]:

- **Data sovereignty,** *"which refers to the degree of control an individual, organization or government has over the data they produce and work with (whether local or online)"*,
- **Technological sovereignty,** *"is defined as the degree of the control the organization has over the technology it uses"*,

11 Kamerbrief over aanbieding Agenda Digitale Open Strategische Autonomie: https://www.rijksoverheid.nl/documenten/kamerstukken/2023/10/17/kamerbrief-aanbieden-agenda-digitale-open-strategische-autonomie-coco-5-oktober
12 Kamerbrief over open strategische autonomie: https://www.rijksoverheid.nl/documenten/kamerstukken/2022/11/08/kamerbrief-inzake-open-strategische-autonomie
13 Based on Reflecties over digitale soevereiniteit https://www.uu.nl/sites/default/files/Moerel%2C%20Timmers%20%282.0%29%20-%20Preadvies%20Staatsrechtconferentie%202020.pdf
14 Achieving digital sovereignty goals with open collaborative technology: https://govinsider.asia/intl-en/article/Achieving-digital-sovereignty-goals-with-open-collaborative-technology
15 Ibid
16 Ibid
17 Digital Security Magazine Atos: https://atos.net/en/lp/digital-sovereignty-cybersecurity-magazine/what-is-sovereignty-and-why-it-does-matter#:~:text=Data%20sovereignty%20and%20technological%20sovereignty,software%2C%20systems%2C%20and%20hardware.

Then for both pillars various questions emerge from a geographical, operational and regulatory perspective (see Figure 1[18]). In addition, cybersecurity is at the heart of data sovereignty and supports techno-logical sovereignty.

These questions can be summarized in to 3 main questions that we will cover in this report:

- **What are the most important suppliers of these technologies?**
- **How dependent are Europe and the Netherlands on non-European suppliers?**
- **What is needed to decrease the dependence and increase digital sovereignty in Europe and the Netherlands?**

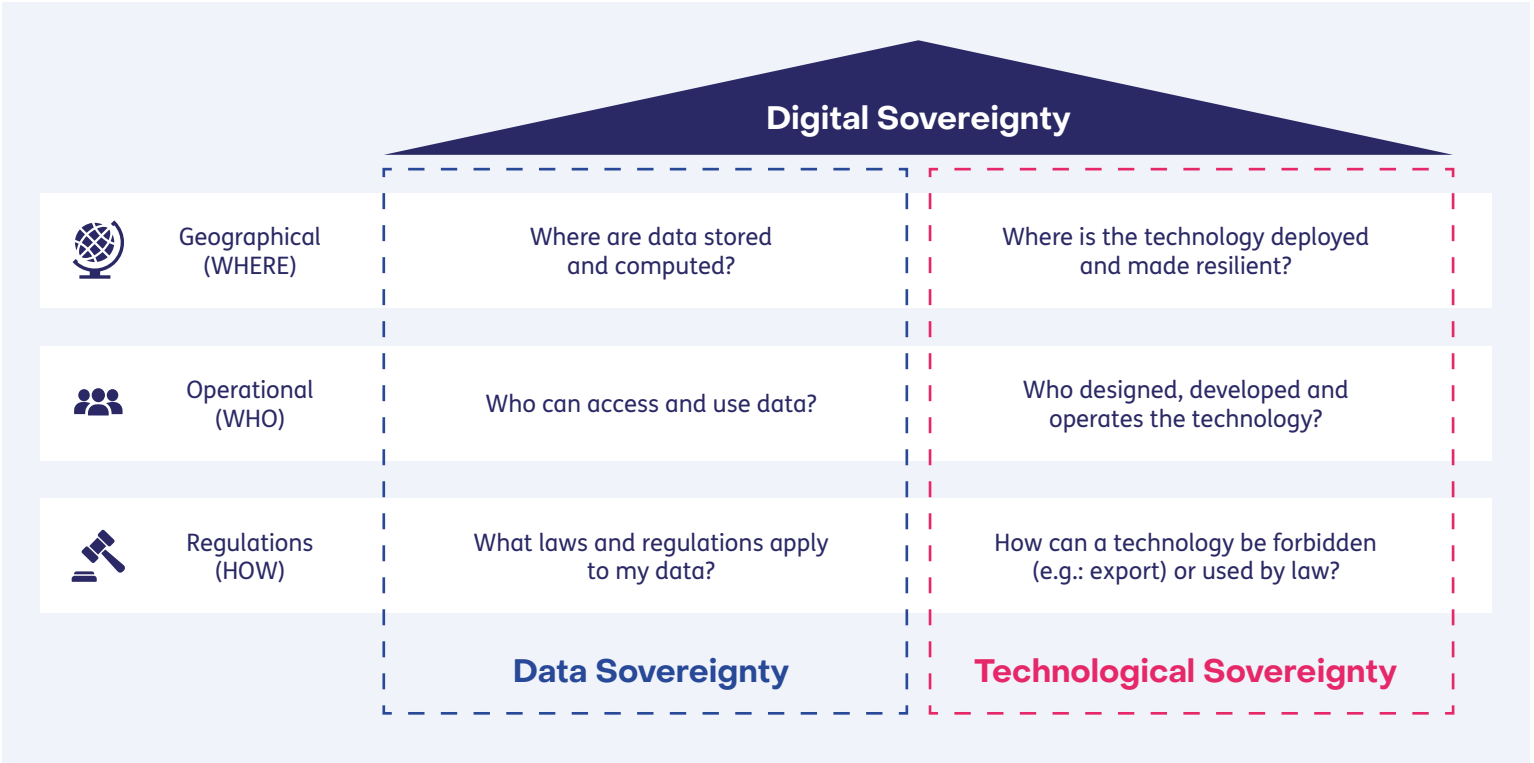

Figure 1 *What is digital sovereignty and why does it matter?*

1.1 Aim and target group

This paper builds on our digital sovereignty paper from 2022, which clarified the term digital sovereignty and identified some first activities on this topic. The aims of this paper are to:

Provide an updated overview of the state of play of digital sovereignty in Europe and the Netherlands based on different perspectives economic, societal, company and cybersecurity perspective.

Indicate what measures could be applied by the Triple helix; policy makers, companies and Research Institutes to collectively increase the digital sovereignty of Europe and the Netherlands.

1.2 Reading guide

In Chapter 2 we describe the state of play of digital sovereignty in Europe and the Netherlands per digital technology layer. Chapter 3 gives insights in to the digital sovereignty from different perspectives; e.g. Economic, Societal, Cybersecurity. Chapter 4 discussed measures to increase digital sovereignty from three perspectives (socio-economic, companies/organizations, cybersecurity). We end in Chapter 5 with the conclusions and recommendations.

18 What is sovereignty and why does it matter? https://atos.net/en/lp/digital-sovereignty-cybersecurity-magazine/what-is-sovereignty-and-why-it-does-matter

2. State of play based on the technology stack model

In order to describe the state of play of the digital sovereignty of the EU and the Netherlands on the world stage, the question is: *What entity is it in the digital Domain that we will focus on?* The EU has first of all a huge technology sector, and its internet coverage is among the broadest and fastest in the world. On the other hand, there is absence of EU companies among the Big Tech companies.[19] *So the question is how to weigh these different observations?*

As indicated in various studies[20], the available data sources provide an ambiguous picture on digital sovereignty. This has to do with the complexity and diversity of the digital domain. It involves microchips and semiconductors, networks and connectivity, cloud and edge infrastructures and much more. Therefore, we build on the technology stack model of Freedomlab and the technology layer model from our previous paper of 2022[21] (See Figure 2[22]). In the next sections we will discuss for each of the technology layers the status of digital sovereignty of

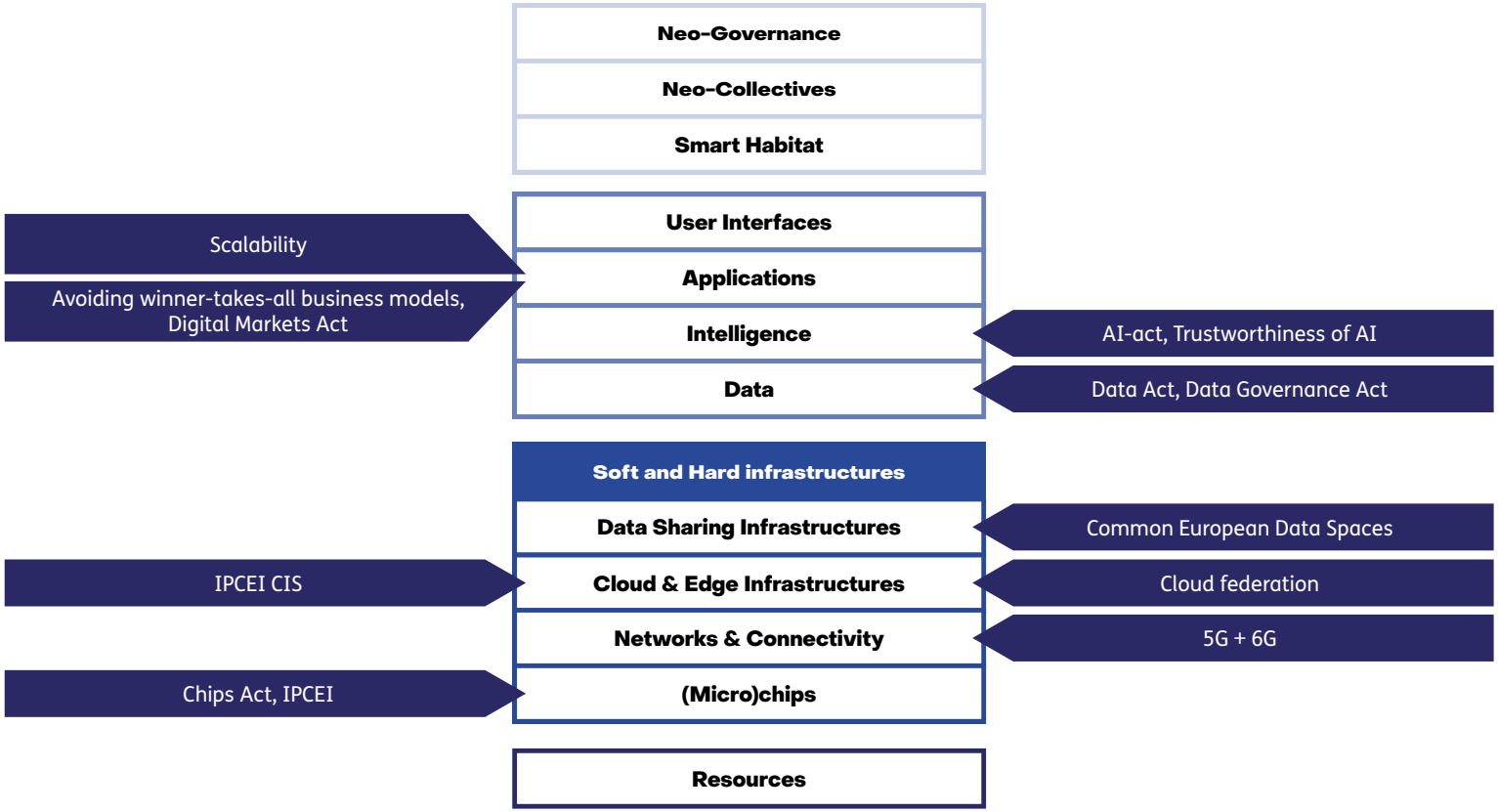

Figure 2 *Technology Stack Model*

19 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink

20 Ibid

21 Bridging the Dutch and European Digital Sovereignty gap: https://publications.tno.nl/publication/34639349/urAkBu/TNO-2022-R10507.pdf

22 Figure 2 is based on the Stack Model of Freedom lab and contains elements of the model that we developed in our study from 2022.

the EU and the Netherlands seen from the global perspective by explaining the dependence on the various stakeholders and countries. The global perspective in this context means mainly Europe, the US and Asia since the most important suppliers for the digital stack layers come from these regions. For the societal oriented layers such as Neo governance we focus on the impact that a lack of digital sovereignty on the technical layers has on these more societal oriented layers. For the technical layers we look at this from three perspectives: 1. R&D, 2. Commercialization and 3. Policy and regulation.

The dark blue boxes on the left and right side of Figure 2 provide examples of policy instruments (e.g. IPCEI CIS), regulation (e.g. Data Act), technologies (e.g. 5G & 6G) and other topics (e.g. scalability, avoiding winner takes all and stimulating business models) that are relevant to increase digital sovereignty. These topics will be covered in the next sections.

2.1 Resources

At the lowest layer of the stack is the resource layer consisting of basic materials including rare earth metals.[23] Although digital systems can reach virtual heights, ultimately, they remain grounded on a material basis. Every system consists of resources, such as standard elements as steel, glass, silicon, gold, but also new materials such as graphene.[24] Critical raw materials are indispensable for a wide set of strategic sectors including the net zero industry, the digital industry, aerospace, and defence sectors.

R&D

There is a lot of research ongoing on the resource layer. Especially on critical raw materials by the EU[25], the OECD[26] and various Member States. Also the US conducted a critical materials assessment.[27] So does China that analyzed and categorized materials and minerals based on their strategic-ness.[28]

Other types of research that take place inside and outside the EU by many research institutes (for more details see the reference)[29] has to do with recycling of resources in order to reuse scarce materials or it focusses on alternative materials.

Besides that there is a scientific stream called materials informatics which is very useful for this layer. Materials informatics is the use of data and AI methods to better understand the use, selection, development, and discovery of chemicals and materials.[30] However, for this type of research there are still some challenges due to a lack of data volume.[31]

The most important research institutes working on this are[32]: Stanford University, Northwestern University, MIT, the National Institute of Standards and Technology (NIST), the National Institute for Materials Science (NIMS), the University of Cambridge, and the University of Toronto.

Commercialization

The global landscape of material supply shows a clear picture of Chinese dominance. Although the four largest producers of lithium are from Chile and Australia, Bolivia and Argentina, the two largest lithium companies are Chinese (Jiangxi Ganfeng Lithium and Tianqi Lithium).[33] With regard to cobalt, the Democratic Republic of Congo has more than 50% of the world's proven reserves and is also the largest producer of cobalt. However, China is a large investor in the mining sector of the Democratic Republic of Congo. Globally, Chinese companies

23 Freedom lab Introduction to the stack: https://www.freedomlab.com/posts/an-introduction-to-the-stack
24 Ibid
25 Study on the Critical Raw Materials for the EU. See: https://www.rtlnieuws.nl/sites/default/files/content/documents/2023/07/04/Study%202023%20CRM%20Assessment%20%281%29.pdf
26 Supply of critical raw materials risks jeopardising the green transition. See for instance: https://www.oecd.org/newsroom/supply-of-critical-raw-materials-risks-jeopardising-the-green-transition.htm
27 For details about the assessment: https://www.energy.gov/sites/default/files/2023-07/doe-critical-material-assessment_07312023.pdf
28 Chinese assessments of "critical" and "strategic" raw materials: Concepts, categories, policies, and implications
29 See Waste And Recycling Research Institutes | Environmental XPRT (environmental-expert.com)
30 Material Informatics: https://luxresearchinc.com/blog/materials-informatics-key-players/
31 Ibid
32 Ibid
33 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink

control nearly half of all production of refined cobalt.[34] China is most dominant when it comes to rare earth metals. In 2021, the country was responsible for 60% of global production of these materials.[35] China's dominance in this market has led to responses from other countries, causing a decline in China's global market share.[36]

Although European countries such as Poland and Germany have large reserves of several metals, their share in global material production is small.[37] Over the years, European countries have been phasing out their mining industries as a result of social and environmental concerns and undercutting of the market by China (allegedly based on extensive state support and possibly dumping). This has currently left them dependent on foreign actors and this could lead to a clash between strategic concerns and social and environmental concerns.[38]

Policy and rewgulation

The EU has developed policies to reduce its foreign dependence ('de-risking') and increase economic security. It has put forward the Critical Raw Materials Act (CRMA), developed the European Raw Materials Alliance (ERMA)[39], monitors and develops further strategies for the increasing number of critical raw materials and establishes strategic partnerships with third countries such as Canada in 2020 and with the Democratic Republic of Congo in 2023 on sustainable raw material.[40, 41] CRMA contains a comprehensive set of actions to ensure the EU's access to a secure, diversified, affordable and sustainable supply of critical raw materials.[42] It aims to match similar policy initiatives by countries such as the United States or Japan.

2.2 Soft and Hard Infrastructures

In this section the soft and hard infrastructure layers are discussed. On the soft infrastructure layer, are the modular software building blocks that relate to the direct control, connection and virtualisation of hardware (e.g. firmware, network protocols, kernels, operating systems and middleware), the development, management and use of databases, the organisation of the business logic or the way information is presented to the user (presentation layer or front-end).[43] This layer provides the virtual semi-finished products for software development.[44]

In addition to the soft infrastructure there is the hard infrastructure layer, that consists of all the hardware elements defined as infrastructure. For instance for a smartphone, if we open it up, we find the screen, sensors, battery, chips, etc.[45] In general, think of hardware for storage (e.g. hard drives, solid state drives, magnetic tape), computing power (CPU, GPU), transmission (5G antennae, fibre optic cables) and measurement (optic sensors, microphones).[46]

34 Finnish Institute of International Afairs. (2021). The geopolitics of the energy transition: Global issues and European policies driving the development of renewable energy. Accessible at: https://www.fiia.fi/en/publication/the-geopolitics-of-the-energy-transition?read
35 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
36 Ibid
37 Ibid
38 Pitron, G. (2020). The rare metals war—the dark side of clean energy and digital technologies, Scribe, Victoria
39 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
40 Finnish Institute of International Affairs. (2021). The geopolitics of the energy transition: Global issues and European policies driving the development of renewable energy. Accessible at: https://www.fiia.fi/en/publication/the-geopolitics-of-the-energy-transition?read
41 Critical Raw Materials Act: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1661
42 Critical Raw Materials Act: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1661
43 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
44 Ibid
45 Freedom lab Introduction to the stack: https://www.freedomlab.com/posts/an-introduction-to-the-stack
46 Ibid

In the next sections (2.2.1-2.2.4) the following soft and hard infrastructures will be discussed in more detail: (Micro) chips, Networks and Connectivity, Cloud & Edge Infrastructures and Data Sharing Infrastructures.

2.2.1. (Micro)chips

The layer of (Micro)chips or semiconductors involves complex supply-chains and a wide variety of chips from more generic to highly specialized, allowing to store massive amounts of data, process data (computing), or enable interaction (e.g. moving sensor data to the computer).[47] Worth mentioning because of their fast rising importance are AI chips, that are tens or even thousands of times faster and more efficient than conventional 'general purpose' chips for training and inference of AI algorithms.[48]

Some semiconductor companies play a diverse set of roles in the supply chain for chips but most of them are highly specialized, but no single company or country is currently capable of performing on its own all roles in the supply chain for all types of semiconductors required for a modern economy.[49] Leading chip sellers routinely have tens of thousands of suppliers distributed around the globe, and some suppliers are the only companies in the world that possess their technological capabilities at specific performance levels.[50]

R&D

The US and Asia have increased their share of global semiconductor R&D over the last ten years at the expense of Europe.[51] Despite political and national security concerns over the US share of chip manufacturing the American companies continue to account for more than 50% of chip industry R&D expenditure, the market analyst reckons.[52] About 55.8% of worldwide semiconductor industry R&D spending in 2021 was by companies headquartered in the American region—and a large part of that coming from Intel (19%, or $15.2 billion last year). This has increased marginally from 54.5% over the previous ten years.[53] These large investments are mainly done by fabless companies (e.g. (Qualcomm, Broadcom, Apple, NVIDIA), who develop a lot of IP, but produce in Taiwan and Korea.[54] In the meantime the R&D spending of Asian companies – including wafer foundries, fabless chip suppliers, and integrated device manufacturers (IDMs) – exceeded 29% of the worldwide total in 2021.[55] This is a jump up from 18% in 2011.[56] Europe and Japan are now down in single-digit percentages with Japan falling the strongest.[57]

Even though R&D in the existing semiconductor sector is flourishing, there are signs that Moore's law is reaching its limits.[58] This is not purely limited to computing power, but also includes growing concerns regarding the energy consumption of large data centres. That requires energy efficient chips, a smarter design and the use of other more energy efficient materials.

47 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
48 AI Chips: What They Are and Why They Matter https://cset.georgetown.edu/publication/ai-chips-what-they-are-and-why-they-matter/
49 Mapping the Semiconductor Supply Chain: The Critical Role of the Indo-Pacific Regionhttps://www.csis.org/analysis/mapping-semiconductor-supply-chain-critical-role-indo-pacific-region
50 Mapping the Semiconductor Supply Chain: The Critical Role of the Indo-Pacific Regionhttps://www.csis.org/analysis/mapping-semiconductor-supply-chain-critical-role-indo-pacific-region
51 IC Insights: US chip suppliers dominate R&D spending ... (eenewseurope.com)
52 Ibid
53 Ibid
54 Based on expert input
55 IC Insights: US chip suppliers dominate R&D spending ... (eenewseurope.com)
56 Ibid
57 Ibid
58 'Moore's Law's dead,' Nvidia CEO Jensen Huang says in justifying gaming-card price hike - MarketWatch

Commercialization

The development of chips is a process that consists of the following steps[59]:

1. chip design,
2. the materials, manufacturing equipment, etc. and
3. semiconductor manufacturing.

The US is still the leading country in the first two steps. Europe is leading with its Dutch company ASML in machines that enable semiconductor manufacturing. ASML is the sole supplier in the world of extreme ultraviolet lithography (EUV) photolithography machines that are required to manufacture the most advanced chips.[60] EUV stands for extreme ultraviolet, a short wavelength of light to print small, complex designs on microchips in large quantities.[61] Former ASML CEO Peter Wennink said the company has been bringing down semiconductor prices since it was founded 38 years ago and will keep doing so *"for the next couple of decades."* [62] *"The world needs more chips,"* Wennink told. *"So we need to make more machines, which, by the way, will keep growing in average selling price as long as we can drive the cost per transistor down."* [63]

The US is losing ground in the field of manufacturing. Its share of global production declined from 37% in 1990 to 12% in 2021.[64] Whereas China was in 1990 responsible for 1% of global semiconductor manufacturing, it currently surpasses the US with a share of 15% in volume.[65] Advanced chips all come from Taiwan and a few from Samsung and a little from Intel/ Micron/Hynix.[66]

Leading Chinese companies are now producing more advanced chips.[67] Its flagship Semiconductor Manufacturing International Corporation (SMIC) ranks among the top 5 foundries in the world and rivals the American company Intel. Huawei's subsidiary HiSilicon became the first Chinese company to reach the top ten list of semiconductor companies.[68]

Next to the US and China, other Asian countries also have important manufacturers of chips.[69] From 1990 to 2021, Japan's share declined from 17% to 15%. The share of South Korea increased from 13% to 21%.[70] However the Taiwanese company TSMC, is world leader in the manufacturing of advanced chips.[71] Various Asian countries are important for the US strategy that aims to build supply chains that excludes China, while cooperating more with Taiwan, South Korea, and Japan.[72]

The EU share has also declined rapidly over the decades. Whereas in 1990, the EU was responsible for 24% of global manufacturing, just behind the US, it currently ranks 6th by manufacturing at 9%.[73]

59 Allison, G., Klyman, K., Barbesino, K., & Yen, H. (2021). The great tech rivalry: China vs the U.S., Belfer Center for Science and International Afairs, Harvard Kennedy School, accessible at: https://www.belfercenter.org/publication/great-tech-rivalry-china-vs-us
60 ASML is the only company making the $200 million machines needed to print every advanced microchip. https://www.cnbc.com/2022/03/23/inside-asml-the-company-advanced-chipmakers-use-for-euv-lithography.html
61 Ibid
62 Ibid
63 Ibid
64 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
65 Ibid
66 Based on expert input.
67 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
68 Ibid
69 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
70 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
71 Ibid
72 Business Standard 2022
73 Ibid

The fabrication of **next-generation integrated photonics and quantum computing chips** might provide new opportunities but will require modifying existing production lines due to the introduction of exotic materials and new design processes. This implies the need for pilot lines as a first step towards commercialization of these technologies, such as the European Qu-Pilot[74] and JePPIX[75] initiatives.

Policy and regulation

Responding to the declining market share and the digital sovereignty concerns, the European Commission launched the EU Chips Act in February 2022. It has the target to increase the EU share in manufacturing of advanced semiconductors over the next decade. In order to do that the Act focuses on[76]:

1. strengthening fundamental research,
2. building production capacity,
3. developing a framework to increase production,
4. addressing shortages in skills and talent, and
5. developing an in-depth understanding of global semiconductor supply chains.

Additionally, it also includes a forward-looking part on the development of design libraries as well as production and testing facilities for the manufacturing of integrated photonics and quantum computing chips.[77] Besides that fabrication facilities of Intel and TSMC will be built in Germany.[78]

Next to that the IPCEI (Important Project of Common European Interest) on Microelectronics is part on the EUs strategy to strengthen the digital sovereignty on this layer. This IPCEI is amongst others focusing on energy efficient chips and power semiconductors.[79] The IPCEI allows the participating countries to support transnational cooperation projects with major synergies in microelectronics – for maintaining and further expanding European competencies in this field.[80] They also ensure that the entire microelectronics value chain is reliably available to local players.[81]

We can conclude about this layer of the digital stack that the EU's share in the chips industry has been declining, but that it still is a considerable developer and producer of chips.[82] As a result, the EU has strong capacities it can build on[83] with the biggest strengths in equipment, notably ASML in the Netherlands.[84]

2.2.2. Networks and Connectivity

The next layer that we consider is the networks and connectivity layer. This layer concerns the infrastructure for the connectivity of digital technology. This infrastructure consists of the following elements[85]: Telecommunications (mobile networks) for cable and wireless networks, underseas internet cables and satellite technology.

R&D

R&D for networks and connectivity is mainly focusing on next generations of telecom and satellite technology, but also on the connectivity based on future oriented technologies such as quantum. China has a strong lead in **5G and 6G mobile networks** 'high-impact research output' such that there's a high possibility of it establishing a global monopoly in

74 Homepage - QU-PILOT : QU-PILOT
75 Services - Jeppix
76 Regulation (EU) 2023/... of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act) (europa.eu)
77 Ibid
78 German budget woes threaten chip fab funding • The Register
79 About the IPCEI: https://www.ipcei-me.eu/what-is/
80 Ibid
81 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
82 Ibid
83 Ibid
84 Based on expert input.
85 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink

this area.[86] In new 5G and 6G radio, some experts designates China's lead as "high-risk," meaning it is a long way ahead of its closest competitor and that it is home to most of the world's leading research bodies in that field.[87]

The US holds the preeminent global position in space research including **satellites** due to its long-term, steadfast investments in space R&D and its strategic partnerships and collaborations.[88] The US has historically been the dominant power in the space sector. However, Beijing's significant investment in and development of its own technology in this field have positioned China as a rising challenger for the US.[89] China has set an ambitious agenda to transform into a world-leading space power by 2045.[90] China has invested heavily in research and development (R&D). While space technologies like communications satellites underpin much of modern life, a handful of countries have the capability to indigenously launch payloads into space.[91] China sits among this elite group of spacefaring nations.[92]

More **towards the future,** there is growing attention for R&D and proof of concept deployment of quantum communication networks that provide new opportunities. These provide inherent security through the underlying physical properties of quantum particles, as well as a means to connect remote quantum devices. The ultimate goal is to establish a so-called quantum **internet**, which co-exists with the existing internet infrastructure.[93] China is leading in some parts of this development, for example through the establishment of a satellite-based quantum communication link in 2020[94] and more recently through their national wide-area quantum communication network, spanning over 10,000 km.[95] Nonetheless, the EU is still at the forefront of quantum internet R&D with initiatives such as the Quantum Internet Alliance[96], and is concretely working on the roll-out of quantum communication infrastructure through the EuroQCI initiative.[97] As part of the latter, in the coming two years the QCINed project will deploy the first metropolitan scale quantum communication networks in the Netherlands.[98]

Next to quantum, **AI** fulfils also a strong role on this layer. By leveraging AI, communication service providers (CSPs) can manage for instance increased complexity, improving the customer experience while maintaining high network performance.[99] By analyzing network traffic patterns and optimizing resource allocation, AI can boost throughput and reliability.

It also works the other way around since 6G also strengthens AI based applications. When looking at the 6G visions from e.g. ITU (International Telecommunication Union)[100] 6G provides a whole platform of AI based applications (e.g. for autonomous vehicles, remote surgeries etc.).

86 Okano-Heijmans M, Gomes A., Kono D., (2023), Strengthening digital economic security in Europe, Promote, Shape, Regulate and Protect, please! A study for the Dutch Ministry of Economic Affairs and Climate Policy: https://www.clingendael.org/sites/default/files/2023-10/Report_Strengthening_digital_economic_security_in_Europe.pdf
87 Ibid
88 NATIONAL LOW EARTH ORBIT RESEARCH AND DEVELOPMENT STRATEGY: https://www.whitehouse.gov/wp-content/uploads/2023/03/NATIONAL-LEO-RD-STRATEGY-033123.pdf
89 China and Brazil's Cooperation in the Satellite Sector: Implications for the United States? https://www.airuniversity.af.edu/JIPA/Display/Article/3428204/china-and-brazils-cooperation-in-the-satellite-sector-implications-for-the-unit/
90 How is China Advancing its Space Launch Capabilities? https://chinapower.csis.org/china-space-launch/
91 Ibid
92 Ibid
93 Quantum internet: A vision for the road ahead | Science
94 China Reaches New Milestone in Space-Based Quantum Communications - Scientific American
95 Microsoft PowerPoint - Wei_Qi_Session1_Qi_rev1.pptx (etsi.org)
96 Quantum Internet Alliance
97 The European Quantum Communication Infrastructure (EuroQCI) Initiative | Shaping Europe's digital future (europa.eu)
98 QCINed | Quantum Delta NL
99 The full value of AI for telecom networks - Ericsson
100 Based on expert input.

Commercialization

When focusing on commercialization, the key issue in the **telecommunication (mobile networks)** is the rollout of the next generation of 5G networks that increase internet speed a 100-fold, but also to improve the reliability of networks. The global geopolitical battle over this layer got much attention with concerns over infrastructure supplied by the Chinese company Huawei.[101] Over the years, it has become a leading player in the development of telecommunications infrastructure around the world and also in many western countries. Under American President Trump, the concern increased over the economic effects, as well as the security issues of telecommunications infrastructure developed by this company. In May 2019, Trump blacklisted Huawei.[102] The US policy did hurt the company's business and has led several European countries to also ban the company entirely or from the more privacy sensitive parts of their telecommunications networks. Globally however, it remains a strong company with cutting-edge technology. European companies spearheaded the rollout of 3G networks and the EU was well positioned with 4G. With 5G, American pressure notwithstanding, it might still be Chinese companies.[103] This country is currently by far the largest builder of the new generation of networks.[104]

The US and Europe are far behind. In 2020, China had 150 million 5G users, the US had only 6 million. While the American companies Lucent (currently part of Nokia) and Motorola had a 25% market share in telecommunications in 2000, they now disappeared from the list of largest networks companies. In 20 years, Huawei's share jumped to 28%, making it the global leader.[105] The political decision to ban Huawei thus slowed its global reach, but Chinese companies remain at the forefront of building 5G-networks, which also gives the country an edge in developing the technology solutions that this new generation of network technology enables.[106]

There is one technology trend in the industry that could change the balance in the current value chains for telecom networks: Open RAN (Open Radio Access Network).[107, 108] With current network technology there is a high level of integration of infrastructure, which gives an advantage to companies that can provide all the required technology. Open RAN is a new type of architecture that makes telecommunication infrastructure more modular. This means different companies can more easily provide different parts of the infrastructure. The advantage of leading companies such as Huawei that can provide entire infrastructures might thus be weakened. Open RAN is starting to mature, for instance, Ericsson has been awarded a major contract to supply this to AT&T over the next 5 years.[109]

The EU's position in the telecommunication infrastructure is actually quite strong.[110] The US no longer has leading companies in this field, but Amazon and Microsoft are starting to build up a position in this area.[111] Huawei's two main competitors are the European companies Nokia and Ericsson. These two European companies are still large players in the market and provide competitive services.

To enable connectivity between regions globally, another element of network infrastructure are **undersea (submarine) internet cables.** Across the globe, there

101 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
102 Hussein, S. (2019). Huawei ban in the US: Projected consequences for international trade. International Journal of Commerce and Economics, 1(2).
103 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
104 Ibid
105 Hillman, J. E. (2021). The digital silk road: China's quest to wire the world and win the future. New York: HarperCollins.
106 Ibid
107 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
108 Status Open RAN technologie en aanbevelingen; https://open.overheid.nl/documenten/ronl-449dc006720f96246b604559cb11d9802a460f9a/pdf
109 AT&T to Accelerate Open and Interoperable Radio Access Networks (RAN) in the United States through new collaboration with Ericsson: https://www.ericsson.com/en/press-releases/2023/12/att-to-accelerate-open-and-interoperable-radio-access-networks-ran-in-the-united-states-through-new-collaboration-with-ericsson.
110 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
111 Based on expert input.

are more than 400 cables running along the seafloor, carrying over 95% of all international internet traffic.[112]

Two types of companies are important in this area:

1. Companies producing and laying cables such as America's SubCom, Japan's NEC Corporation, France's Alcatel Submarine Networks and China's HMN Tech.[113]
2. Companies operating and owning them. Years ago, submarine cables were first owned by telecommunication companies that would together form a consortium of all the parties interested in using these submarine cables.[114]

Over time and as the internet grew in the mid to late 90s, more companies saw the potential of investing in the infrastructure that enabled the global internet to take off. Countries around the world to recognize that submarine cables were becoming part of critical infrastructure for governments and the private sector.[115] In recent years, Big Tech companies such as Google, Meta, and Amazon have become prominent investors in new cables.[116]

It is important to notice that Microsoft, Meta, Amazon and Alphabet (parent company of Google) have captured the submarine cable market and are becoming the largest shareholders.[117] Before 2012, the organizations used less than 10 % of all submarine cables worldwide.[118] This increased to at least 66%.[119] Recently, concerns have been rising about the vulnerability about submarine cables.

Concerning the **satellite infrastructure,** which is relevant for applications such as communication, monitoring and intelligence, there are satellite vendors and operators. Examples of important vendors who manufacture satellites for communication are: Space-X (US), Airbus (EU), Thales (France).[120] Examples of important operators are Eutelsat (France) /Oneweb (UK), Viasat (US), Immarsat (UK).[121] The US satellite operators are launching big constellations, while there are few European satcom operators that are so big.[122] That means that the US is the clear global leader.[123] The most important new trend in this field is low Earth orbit (LEO) satellites that are cheaper and that fly at a lower altitude than conventional satellites.[124] American vendors such as Space X (US), Boeing (US), and Northrop Grumman (US) are leading this new connectivity technology.[125] However, the European Airbus is also involved in producing LEO satellites[126] as well as Thales, which is also European, and is leading the 3GPP standardization of 5G satcom integration.[127] At the same time, it is clear that China is increasing its share in the market by launching satellites for connectivity. Space is one of the focus

112 U.S. and China wage war beneath the waves – over internet cables. https://www.reuters.com/investigates/special-report/us-china-tech-cables/
113 Inside the subsea cable firm secretly helping America take on China: https://www.reuters.com/investigates/special-report/us-china-tech-subcom/
114 Diving Deep into Submarine Cables: The Undersea Lifelines of Internet Connectivity | Kentik Blog
115 Ibid
116 Ibid
117 'Big tech conquers internet infrastructure, wipes out telco providers: https://www.techzine.eu/news/infrastructure/71312/big-tech-conquers-internet-infrastructure-wipes-out-telco-providers/
118 Big tech conquers internet infrastructure, wipes out telco providers: https://www.techzine.eu/news/infrastructure/71312/big-tech-conquers-internet-infrastructure-wipes-out-telco-providers/
119 Ibid
120 Space Impuls: https://spaceimpulse.com/2023/10/19/european-space-companies/#:~:text=This%20industry%20is%20dominated%20by,especially%20prominent%20European%20satellite%20manufacturers.
121 Top Satellite Communication Companies of 2020 – List of Satellite Operators Leading the Global Market https://blog.bizvibe.com/blog/top-satellite-communication-companies
122 Based on expert input
123 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
124 Ibid
125 Ibid
126 Ibid
127 Based on expert input

points in the countries Made in China 2025 strategy and features prominently in the last few Five-Year Plans.[128] The EU announced in early 2023 that it will launch its own satellites constellation for communication and internet – IRIS2, the European Starlink[129], which is focusing on governmental users and businesses.[130] It should be fully operational by 2027.[131]

When focusing on the **long term future perspective of communication** we see that quantum communication networks are under development. Given that the first users of quantum communication networks will most likely be governments and critical infrastructure providers, there is a growing push to solely use EU-based suppliers for the hardware components of these networks. The current market leaders for certain types of components are Toshiba (Japanese) and IDQuantique (Swiss), but there is a growing base of SMEs in the EU that can also provide key components such as Q-Bird, KEEQuant and LuxQuanta.

Policy and regulation

On this layer there is a substantial support from the EU as well as on national level. We will explain this for each of the 3 underlying technologies of this layer.

For the **telecommunication networks** several host states around the world, particularly in North America and Europe, have taken restrictive measures against foreign telecommunications equipment manufacturers as part of their 5G rollout, including most notably Chinese companies such as Huawei and ZTE.[132] Besides that there is a debate in the EU about policy measures to protect industry champions and some people have even suggested that if the telecommunication companies Nokia and Ericsson were German or French instead of Scandinavian, there would already have been more policy to support them.[133] These champions could function as control points. *'Control points' are defined as unique business activities that are difficult (or impossible) for players in the value chain to avoid".*[134] But they are also defined from a broader perspective *'as crucial links in value chains that are difficult to replace and that are in combination very knowledge intensive.*[135] Such links could be fulfilled by companies/ champions, products and applications.

EU policies include:

1. Active 5G and 6G R&D investment policy e.g.:
   - EU based Smart Network and Services is 900 M euro,
   - The German program is 700 M euro,
   - Dutch Future Network Services is 203 M euro,
   - In Spain it is 205 M euro,
   - Italy is 118 M euro,
   - France is 735 M euro,
   - Finland is 2 programs with 130 M euro and 20 M euro.
2. A 5G Security Recommendation (which is soft law as the EU has a limited mandate for hard law related to national security).
3. There is a White Paper in preparation for a Digital Networks Act, planned for February 21 2024.

Concerning the **underseas internet cables;** The EUs executives wants to help invest in "cable projects of European interest" that would reduce its reliance on too few undersea internet connections and make it less vulnerable to sabotage.[136] The EU push is expected in early 2024 as part of a new strategy to boost its telecom sector and internet infrastructure.[137]

128 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
129 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
130 IRIS² Secure Connectivity Programme: https://defence-industry-space.ec.europa.eu/eu-space-policy/iris2_en
131 Ibid
132 Standards of Protection: The State's Sovereign Right to Regulate and its Limits https://globalarbitrationreview.com/guide/the-guide-telecoms-arbitrations/second-edition/article/standards-of-protection-the-states-sovereign-right-regulate-and-its-limits
133 Benner, T. (2021). Seven lessons from the German 5G Debate, Global Public Policy Institute. Accessible at: https://gppi.net/2021/12/30/seven-lessons-from-the-german-5g-debate
134 NXTGEN Hightech
135 Bree van T., Bastein T., Vierhout J., en Bolhuis W., (2023) Toekomst van de Nederlandse industrie: link
136 EU looks to boost secure submarine internet cables in 2024: https://www.politico.eu/article/eu-looks-to-boost-secure-submarine-internet-cables-in-2024/
137 Ibid

It will lay the ground word for a new "digital networks act[138]," announced by Internal Market Commissioner Thierry Breton and expected in 2025, that would help not only submarine cables, but also mobile networks and fiber roll-out, edge computing etc., as well as telecoms players to speed up technological advances by easing restrictions and attracting more capital.

Concerning the **satellite technologies;** Internal Market Commissioner Thierry Breton was the one who first proposed the idea and the initial public budget for funding the creation of the aforementioned European satellites for communication and internet.[139] The budget will be 2.4 billion euros, in addition to more than 642 million euros provided by the European Space Agency.[140] However, SpaceX alone is investing 20-30 billion dollar in the American Starlink.[141] This means that the European investment is very low when comparing these budgets.

Finally, **towards the future as far as quantum is concerned** the US will allocate for instance 15 million dollar per year in the period 2023-2027 for quantum networking and communication research and standardization, as part of their 2022 CHIPS and Science Act[142]. This also includes the standardization of post-quantum cryptography protocols. Over the past four years, Europe has invested in quantum technologies with for instance the EuroQCI project, to develop a robust scientific and industrial ecosystem, foster the emergence of national champions and enable the forthcoming implementation of a secure communications network between member states.[143]

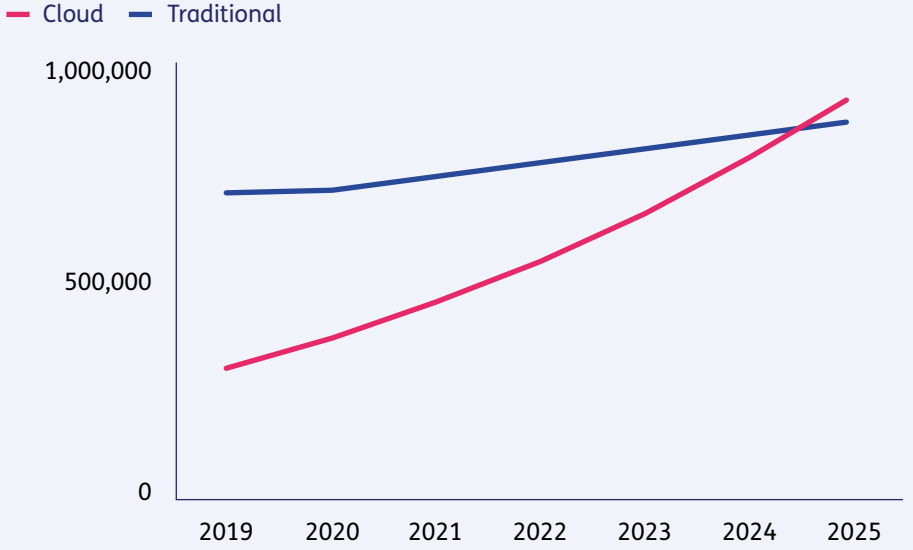

Figure 3 *Shift from On-Premises towards IT Cloud Services*

138 Ibid
139 The EU Will Launch Its Own Satellites Constellation for Communication and Internet – IRIS², the "European Starlink" https://atlas-report.com/the-eu-will-launch-its-own-satellites-constellation-for-communication-and-internet-iris%C2%B2-the-european-starlink/
140 The EU Will Launch Its Own Satellites Constellation for Communication and Internet – IRIS², the "European Starlink" https://atlas-report.com/the-eu-will-launch-its-own-satellites-constellation-for-communication-and-internet-iris%C2%B2-the-european-starlink/
141 Elon Musk touts SpaceX surging internet growth, but still says goal is to avoid bankruptcy | CNN Business: https://edition.cnn.com/2021/06/29/tech/elon-musk-spacex-starlink-scn/index.html
142 Quantum in the CHIPS and Science Act of 2022 - National Quantum Initiative
143 EU invests $200M in quantum technology to secure communications networks - SDxCentral: https://www.sdxcentral.com/articles/news/eu-invests-200m-in-quantum-technology-to-secure-communications-networks/2024/01/

2.2.3. Cloud and Edge infrastructures

The next layer that we consider is the cloud and edge infrastructures layer.

Whereas computation used to happen at local servers and mainframes, a large part of global computation is nowadays moved to the cloud (see Figure 3[144]).[145]

Specialized companies provide these services. Complex cloud services require a lot of computational infrastructure at vast data centers. However, we also see cloud/edge infrastructures that provide specialised resources, next to general purpose computing, to e.g. optimize the handling of streaming services.

Edge computing is a more recent development. It is a distributed computing approach that brings computation and data storage closer to the sources of data.[146]

R&D

The largest R&D investors active in cloud computing are American companies notably Amazon, Microsoft and Google[147]. See Figure 4[148] for the total R&D spending[149] of some of them. They increasingly dominate markets benefiting from a winner-takes-it-all effect that is strong in cloud due to network effects (meaning that the more people use the platform the more attractive it becomes) but also often being accused of lock-in strategies. Their deep pockets means that they also can afford to spend huge amounts on R&D in cybersecurity and AI that get tightly integrated with cloud services, risking to further increase the concentration of power, dominant positions, and consequently increasingly affect digital sovereignty of Europe and the Netherlands.

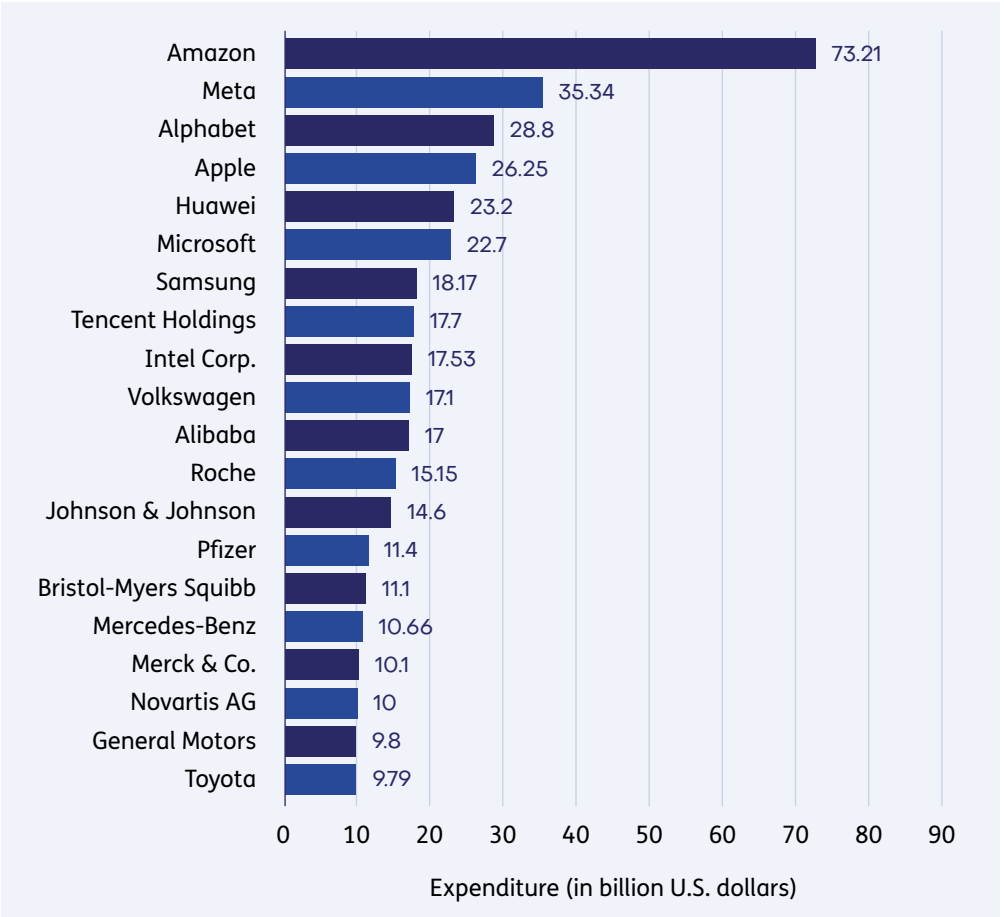

Figure 4 *Total R&D spending tech companies 2022*

144 Gartner, How Cloud Adoption will Opex Budgets
145 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
146 Edge Observatory for Digital Decade – Monitoring the Deployment of Edge Nodes: https://digital-strategy.ec.europa.eu/en/policies/edge-observatory
147 The World Biggest R&D spenders: 27214.jpeg (1200×1200) (statcdn.com)
148 Companies with highest R&D spending worldwide 2022 | Statista
149 This is total R&D spending, so not only on cloud but also on other R&D activities .

Major market players in edge computing are investing a lot of R&D in applications and product portfolios, which will in turn stimulate the edge computing.[150] Companies with the most edge computing patents are from China but also a company such as Intel is in the top list see Figure 5[151, 152]

In Europe network operators[153] see edge computing as an opportunity to monetize their distributed real estate. Network operators often have a quite distributed network infrastructure, with many suitable locations for edge computing. There is also a desire not to only depend on the large cloud providers, but to provide customers a range of cloud options from private cloud to public / hyperscaler cloud. This development is also exemplified by a number of European operators that are developing an open source platform for operator edge cloud.[154]

US operators on the other hand seem to have a stronger strategy of collaborating with hyperscalers for edge services. They are even not only outsourcing cloud functionality for their customers, but also

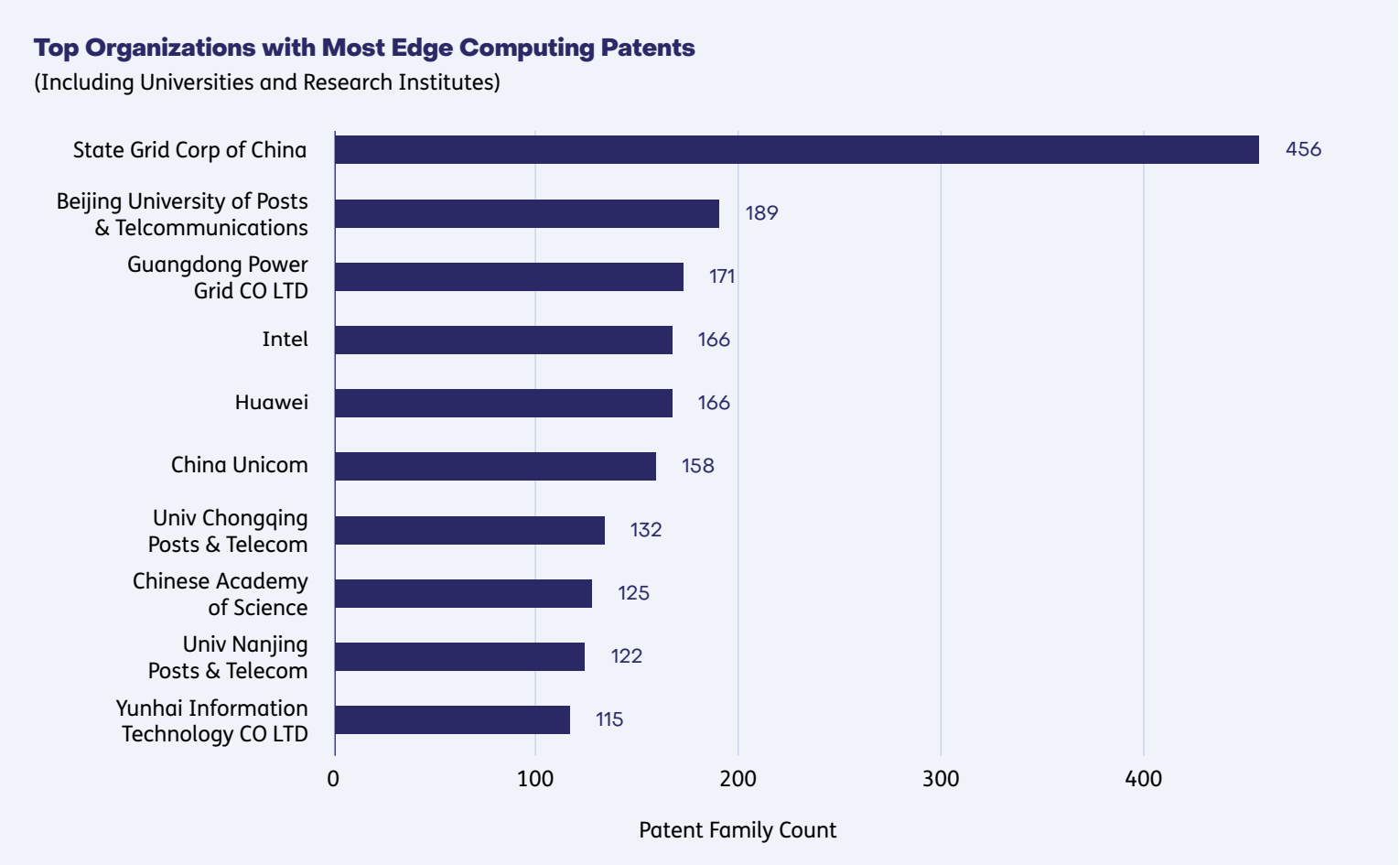

Figure 5 *Top Organisations with Edge Computing Patents*

150 Edge Computing Market overview: https://www.marketresearchfuture.com/reports/edge-computing-market-3239
151 Ibid
152 Top 10 Companies Leading the Research in Edge Computing: https://www.greyb.com/blog/edge-computing-companies
153 e.g. KPN CMD 2023 Presentation
154 Sylva – Linux Foundation Projects Site (sylvaproject.org)

the cloud infrastructure they need for their own operator networks. Verizon and AWS expand 5G mobile edge computing (MEC) coverage to three more locations.[155]

It is important to understand that also the network infrastructure of telecom operators is increasingly cloud based. Telcos expected to invest $1 billion on average in network cloud transformation to enable a future connected world.[156] The question is whether operators will outsource that cloud infrastructure to hyperscalers (seems to be the direction US operators go) or whether they want to use private cloud infrastructures (examples are operators behind the Sylva project[157]).

Towards the future there are on this layer also developments expected based on quantum technology. The current vision for large-scale quantum computing systems is that they will be integrated with existing high-performance computing centres. In Europe, the EuroHPC Joint Undertaking has selected six sites across different EU member states to host quantum computers.[158]

Commercialisation

Cloud is dominated by a trio of Big Tech companies and there are no signs the market is becoming less concentrated.[159] For years, concern has grown about "lock-in" effects. Lock-in occurs when the high cost of switching from one provider of technology to another effectively locks users into their current provider.[160] The ACM (Autoriteit Consument & Markt in the Netherlands) makes a distinction between financial (high data transfer costs if you want take data from the cloud) and technical switching barriers (due to close technical integration between the application and infrastructure) which make switching between clouds an activity that requires a lot of engineering effort. Together both barriers makes it very unattractive to switch between clouds. This poses a particular problem if services of different providers need to work together. Some initiatives are trying to mitigate this by providing solutions to federate a certain layer of a cloud platform[161], but they are not yet commonplace. Hyperscalers are however adopting approaches for cloud federation, but mostly within their own ecosystem focusing on cloud-edge interconnectivity. Besides that Google luckily recently removed its data transfer fees for clients switching to rivals.[162] However, many cloud providers, including Microsoft and Amazon still charge customers based on the amount of data transferred when they switch vendors.[163]

The largest players in the field of cloud computing are American companies. The global leader is Amazon with Amazon Web Services (AWS). According to Statista, in 2021, Amazon had 33% of the global market. Second is Microsoft's Azure service with a 21% market share.[164] Next, on a smaller scale is Google Cloud Platform with 10% market share.[165] That means that these three US companies hold almost two-third of the global market. The first non-US companies in the top list is China's Alibaba with about 6% market share, which is mostly restricted to the Chinese market.[166] Then other US companies like IBM and Salesforce follow. The Chinese company Tencent, the only other non-American company in the list, has a 3% market share.[167]

155 RCR Wireless news rcrwireless.com
156 Verizon 5G MEC is now available in Chicago, Houston and Phoenix: https://www.rcrwireless.com/20210806/5g/verizon-and-aws-expand-5g-mec-coverage-to-three-more-locations
157 Sylva – Linux Foundation Projects Site (sylvaproject.org)
158 One step closer to European quantum computing: The EuroHPC JU signs hosting agreements for six quantum computers (europa.eu)
159 Loosening the Hold of Big Tech on the Cloud: Can the Market (and a Merger) Help? (pymnts.com)
160 Ibid
161 For example: Liqo.io (https://liqo.io) and Rancher (https://www.rancher.com)
162 Google Cloud removes data transfer fees when clients switch to rivals: https://www.reuters.com/technology/google-cloud-removes-data-transfer-fees-when-clients-switch-rivals-2024-01-11/
163 Ibid
164 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
165 Ibid
166 Ibid
167 Ibid

Next to these large global players, in many countries there are smaller European providers such as OVH Cloud or telecommunications companies providing cloud services like Deutsche Telecom and British Telecom.[168] On the global scale, however, there are no European companies. As a consequence, European businesses and governments are strongly dependent on the services of a few American companies.

Content wise there is a strong focus by cloud computing firms on AI. They are aggressively pursuing investments and alliances with **artificial intelligence** startups through their cloud computing arms.[169] The technology behind products including OpenAI's ChatGPT, a chatbot that can converse with users through text, requires enormous amounts of computing power—expensive infrastructure controlled by the same handful of tech giants.[170]

AI startups that need to train AI models have little choice and rush into the arms of large companies offering essential cloud computing at discounted rates and access to the large amounts of capital they need.[171] OpenAI[172] started as a research laboratory co-founded by Elon Musk, to become for-profit in 2019 with a capped approach to profit.[173] This company released the ChatGPT as one of its most famous products and Microsoft publicly committed in 2023 to a multibillion-dollar investment in OpenAI.[174]

Edge computing is also in the hands of the usual suspects such as AWS and Microsoft. But there are also some other players such as ClearBlade, EdgeConneX, Section etc.[175] As mentioned earlier in this section edge computing is also seen as an opportunity for Europe such as for the EU network providers.

When looking at **future solutions** that could change this situation such as quantum technology there are some challenges. Given that building a quantum computer is extremely resource intensive, there are only a few commercial fully integrated systems in the world. The corresponding business model is then to provide access to these systems remotely through a web interface. Leading providers of these services are currently mostly US Big Tech companies such as AWS, Microsoft and IBM, where the latter also builds and controls the underlying quantum computing hardware itself.[176] Even though there are European alternatives, such as PASQAL (originating in France)[177], the underlying platform and resulting applications are generally not at the forefront compared to the system of commercial companies in the US.[178] There is thus a risk that the dominant position of Big Tech companies in the existing digital domain will be extended to quantum computing. This also has to do with the large investments needed for future solutions such as quantum. Looking at the financial situation of companies, these are mainly the Big Tech companies from the US that have a lot of money for such investments.

Policy and regulation

Germany and France took the initiative to respond to this high concentration in cloud dependence with the Gaia-X initiative. Gaia-X's aim is not to create an European alternative to the services of Amazon or Microsoft, but instead focusing on providing a trust framework for digital infrastructures. It is an initiative of technology development, demonstrator pilots and standards development, to enable a data sharing infrastructure with common European standards.[179] Gaia-X-based infrastructure should make

168 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
169 Big Tech companies use cloud computing arms to pursue alliances with AI groups | Ars Technica
170 Ibid
171 Big Tech companies use cloud computing arms to pursue alliances with AI groups | Ars Technica
172 OpenAI: https://www.techtarget.com/searchenterpriseai/definition/OpenAI
173 Ibid
174 OpenAI: https://www.techtarget.com/searchenterpriseai/definition/OpenAI
175 Top Edge Computing Companies to Know: https://thenewstack.io/edge-computing/top-edge-computing-companies-to-know/#:~:text=While%20AWS%20and%20Microsoft%20Azure,%2C%20Section%2C%20and%20many%20more.
176 IBM Quantum Computing | Qiskit Runtime
177 Pulser Studio - PASQAL
178 Can Europe Catch Up with the US (and China) in Quantum Computing? | BCG
179 Tardieu, H. (2022). Role of Gaia-X in the European Data Space Ecosystem. In Designing Data Spaces. Springer, Cham. Accessible at: https://link.springer.com/chapter/10.1007/978-3-030-93975-5_4

it possible for European companies to grow as providers of cloud services in the future.[180]

Next to that European initiative there is DOME, A Distributed Open Marketplace for Europe Cloud and Edge Services[181], to provide cloud edge services over various cloud platforms.[182] As well as IPCEI CIS which was approved in December 2023 as an Important Project of Common European interest for Cloud Infrastructure and Services. This promotes the development of next-generation infrastructures and services.[183] Currently, there are no significant commercial European players in this field. Regulation is a current avenue to shape the market for cloud services while they remain dominated by foreign businesses.[184] Examples of regulation for this layer are:

- EU Data Protection Code of Conduct for Cloud Service Providers[185]: The code defines clear requirements for cloud service providers which covers the processing activities of every type of personal data.
- EU Data Act[186]: On November 9, 2023, the European Parliament adopted the EU Data Act, a new regulation providing harmonized rules on access to data, switching cloud providers and interoperability requirements across the EU.
- EU Cloud rule book[187]: Will provide a single European framework relevant binding and non-binding rules for cloud service users and providers in Europe.

2.2.4. Data sharing infrastructures

The next layer relates to 'data sharing infrastructures'. We consider this a separate layer between cloud/edge and data. The reason for this is the need to have common services in place that enable the trusted sharing of data between parties. Such services can include identification or marketplace services and are especially relevant in situations where large numbers of actors, which might not necessarily know each other, need to share data. This layer can be seen as an orchestration layer.[188] Such data sharing infrastructures enable what is sometimes called 'data spaces'[189, 190] Like on the cloud layer, this layer is currently driven by hyperscalers, providing an integrated cloud data sharing offering.[191] It is the basis for many end-user data sharing applications.[192]

R&D

Traditionally data sharing has concentrated on EDI (electronic data interchange) and the use of shared digital platform for exchanging digital messages. Research has focused mostly on the semantics of data exchange and the setting-up of joint data models and message specifications[193]. In an operational setting this has led to digital business platforms such as SAP Ariba and SupplyOn, which bundle EDI transactions between many organizations in an entire industry or sector.

180 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
181 Dome Marketplace: https://dome-marketplace.eu/
182 Based on expert input.
183 ICPEI CIS: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6246
184 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
185 Belgian DPA Approves First EU Data Protection Code of Conduct for Cloud Service Providers. Privacy & Information Security Law Blog. 2021-05-24. Retrieved 2021-08-26.
186 Almost there: The European Parliament passes the EU Data Act, with new rules for data access, switching cloud providers and interoperability in the EU: Almost there: The European Parliament passes the EU Data Act, with new rules for data access, switching cloud providers and interoperability in the EU | WilmerHale
187 Cloud computing: https://digital-strategy.ec.europa.eu/en/policies/cloud-computing
188 Stolwijk, Punter et al. (2022), Bridging the Dutch and European Digital Sovereignty gap: https://publications.tno.nl/publication/34639349/urAkBu/TNO-2022-R10507.pdf
189 A data space is a distributed system defined by a governance framework that enables secure and trustworthy data transactions between participants while supporting trust and data sovereignty (Glossary DSSC).
190 JRC: "decentralized infrastructures, where diverse actors can share and use data in a secure, reliable and trustworthy manner, following common governance, organizational, regulatory and technical mechanisms"
191 Stolwijk, Punter et al. (2022), Bridging the Dutch and European Digital Sovereignty gap: https://publications.tno.nl/publication/34639349/urAkBu/TNO-2022-R10507.pdf
192 Ibid
193 See for example: VoCol An Integrated Environment to Support Version-Controlled Vocabulary Development https://link.springer.com/chapter/10.1007/978-3-319-49004-5_20

R&D has shifted towards models based on decentralization. Many R&D was put into setting-up of blockchain-technology, whereby transactions were registered in distributed ledger. This would reduce the winner-takes-all tendency of existing digital business platforms, although many business models of blockchain initiatives were based on the issuing of tokens.

Research has further evolved into the topic of data sovereignty and trust: providing individuals and organizations with the ability to control the sharing and use of their own data. The GDPR required organizations to get consent from individuals for the use of their own private data. Data sovereignty takes this further and applies this to other kinds of data too. Notably the International Data Spaces Association (IDSA) has taken-up this topic, setting-up a reference architecture model[194]. Gaia-X has initiated the work on a 'digital clearing house'[195], which – in essence – provides a registry of participants of a data spaces and their underlying attestations. This is aimed at providing an agreed level of trust to participants in a digital ecosystems through trust service providers.

These developments fit in a wider trend towards so-called 'zero trust architectures'. Such infrastructures operate on the premise that no entity within or outside the network is trusted by default. Instead, verification is required from everyone trying to access resources in the network. This can include both data, algorithms and the underlying cloud and computing resources. By integrating zero trust architectures into the fabric of common European data spaces, it becomes possible to enhance data security, privacy, and governance, fostering an environment where data can be shared and utilized effectively while respecting the sovereignty and privacy of all participants – and it becomes easier to accommodate scenarios where data needs to be shared between participants in different jurisdictions or data spaces. This is considered a critical element in the wider data economy[196].

Commercialisation

Key big-tech players have integrated data sharing infrastructures into their cloud offerings. Examples include Salesforce, Amazon S3 and Microsoft Azure. Data sharing services are integrated first of all to onboard organizations into the cloud, e.g. by providing IoT-integration our data onboarding solutions. Secondly tools are provided for data management purposes, e.g. for providing controlled access to data or for developing APIs (Application Programming Interfaces). The focus is on single customers, either a platform player or individual organizations participating in a data ecosystems.

The IDSA has established a certification scheme for their reference architecture model, providing a fabric for the data ecosystem – the data space – itself. This includes both the endpoints of individual organizations as well as the intermediary services necessary for finding, identifying and trusting other partners in the data space.

A small number of companies have started to offer connectors and services based on this. An example is the German spin-off company Sovity.[197] In addition, some organizations have started an open-source initiative under the Eclipse foundation[198], called Eclipse Data Space Components (EDC). To bundle both initiatives the IDSA has announced the creation of a dedicated Eclipse group for managing the Data Spaces Protocol, which is the underlying specification of both the Reference Architecture Model and the EDC[199]. Within the Eclipse community several large players, e.g. Microsoft, are active too. Huawei has announced the availability of Boot-X, which contains their reference implementation of these specifications[200]. This provides these hyperscalers with a platform to introduce these technologies as part of their offering at relatively short notice.

Other players have stepped into this market as well. With an initial focus on the automotive sector the new company Cofinity-X[201] aims to provide services to

194 IDS RAM 4.0 - IDS Knowledge Base (internationaldataspaces.org)
195 Gaia-X Framework - Gaia-X: A Federated Secure Data Infrastructure
196 Zero Trust Architecture (nist.gov)
197 Sovity: www.sovity.de
198 Eclipse Foundation | The Eclipse Foundation
199 Dataspace Protocol - Working Draft - IDS Knowledge Base (internationaldataspaces.org)
200 Boot-X: https://www.boot-x.eu/
201 Home - Cofinity-X GmbH

organizations active in the automotive supply chain. German telco T-Systems has also joined this business through their Data Intelligence Hub.[202] Dutch telco KPN has announced a similar initiative for the Dutch market.[203] These companies either target data space governance bodies and/or participants of a data space.

To support the development of data spaces in key domains, the European Commission has tendered the delivery of open source middleware components, under the title 'Simpl'. This was awarded late 2023 to a consortium led by Eviden (former: Atos). It is likely that this consortium will provide high-TRL reference implementations of components in line with earlier developments of IDSA and Gaia-X. Since these components will become available in open source, they can provide a platform for the software industry to start new commercial offerings. The exact pathway to this is still unclear, as is the detailed scope of work for Simpl in 2024 and beyond. What is clear however is that there are three chunks of development: 1. Simpl Open (developing software), 2. Simpl Labs (providing a playground) and 3. Simpl Live (supporting an initial number of public-sector data spaces).

Policy and regulation

The European Commission and several member states have policies in place to support the development and roll-out of data spaces and the required underlying data sharing infrastructure to provide an alternative for Big Tech. Within the EU projects that are funded under the Digital Europe programme there are three key themes:

- Coordination and support actions in key-domains (e.g. energy, mobility, skills)
- Deployment actions in those domains
- A cross-cutting Data Spaces Support Centre (DSSC) to develop a common blueprint

This is in parallel to the aforementioned Simpl initiative. It is likely that Simpl will adopt the common blueprint of the DSSC and that the various domains will adopt the results of Simpl.

For some domains, such as healthcare, dedicated legislation is in place or has been proposed to set-up the required data spaces (e.g. the European Health Data Space Regulation). In this case deployment and legislation are more closely linked together.

For identity management, the EC has launched the eIDAS 2.0 regulation. A key component of this regulation is the setting-up of so-called qualified trust service providers and electronic wallets for identities. Each member state should have a register of such QTSPs (Qualified Trust Service Providers) and make sure that at least one wallet implementation is available. This provides a key framework for future digital identities. It is expected that similar services will become available for other (non-eIDAS 2.0 regulated) attestations, such as identities of digital twins of equipment – following a similar technological framework.

2.3 Data

Data is the fuel of the digital system and is meant to store, send and process. In the data layer, the precise nature of the data will be defined which is very important for the intelligence layer.[204] For example, on an iPad, the metadata of our photo albums makes it possible to search them with preciseness. A digital system may work with personal data (behaviour, emotions, features) or more contextual data (weather, location, time) or data from more abstract actors (company data, government data). Furthermore, this layer also looks at the volume, variety, reliability and validity of the data collected in a system.[205] These features in turn determine the quality of smart algorithms that are trained on these datasets.

R&D

For R&D purposes, such as innovating with AI access to large data sets is very important. However, unfortunately these data sets are often stored in the silos of Big Tech. Building data sets is very costly. It is therefore important to maximise the value of the data that is available by preserving them and when possible, making them available for reuse. Making a data set available for further research and development means that it is important to keep the data set-up to date by ensuring that researchers contribute with new data. Data obsolescence is a problem.[206]

202 Telekom Data Intelligence Hub
203 Data uitwisseling in de Maakindustrie op grote schaal mogelijk door SCSN, TNO en KPN (smart-connected.nl)
204 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
205 Ibid
206 In-Depth Guide to Data Commercialization in 2023: https://gpai.ai/projects/data-governance/role-of-data-in-ai.pdf

Especially, for AI because accurate AI developments and training of AI models cannot be done based on something which no longer represents the reality. Other major drivers for reuse are cleanliness, accessibility and compliance with the FAIR4 (Findable, Accessible, Interoperable and Reusable) principles.[207] Retaining and continuously improving data helps improve AI models and for monetising, repurposing and recombining data assets that build up over time (which can give rise to new applications or value chains).[208]

Commercialization

Companies in every industry use data to create value and manage data as an asset. They collect and analyse huge amounts of data from various sources. Data enables businesses to make real-time decisions. Businesses have realized that not sharing their data is a fundamental organizational barrier, and organizations are already commercializing their data to generate revenue.[209] Internet of things (IoT), artificial intelligence (AI), and blockchain are the three major technological components contributing to the growth of data commercialization. The top 10 companies active on BIG Data are Amazon, Microsoft, Google, Facebook, Instagram, Netflix, Spotify, IBM, Oracle and VMware.[210] Meaning that basically BIG Tech is active here.

Policy and regulation

The EU's position in data is weaker than both China and the US. This is partly caused by more strict privacy regulation in the EU, but also because there are less comprehensive datasets and there is great fragmentation of datasets across the countries of the EU.[211] The EU put various policy measures and legal documents in place to make our society more data driven and to mitigate the lack of digital sovereignty on this layer. There is first of all the European data strategy which aims to make the EU a leader in a data-driven society.[212] Creating a single market for data based on this strategy will allow it to flow freely within the EU and across sectors for the benefit of businesses, researchers and public administrations.[213] But there is also other legislation such as the:

- **Data act**[214]: with a strong focus on unlocking industrial data, that contains measures to[215]:
  - Enable users of connected devices to access the data generated by these devices and by services related to them.
  - Provide protection from unfair contractual terms that are unilaterally imposed.
  - Provide mechanisms for public sector bodies to access and use data held by the private sector in cases of public emergencies such as floods and wildfires, or when implementing a legal mandate where the required data is not readily available through other means.
  - Provide new rules that grant customers the freedom to switch between various cloud data-processing service providers.
  - Promote the development of interoperability standards for data-sharing and data processing, in line with the EU Standardisation Strategy.
- **Data Governance act**[216]: is a cross-sectoral instrument that aims to make more data available by regulating the re-use of publicly/held, protected data, by boosting data sharing through the regulation of novel data intermediaries and by encouraging the sharing of data for altruistic purposes.

207 Ibid
208 Ibid
209 https://research.aimultiple.com/data-commercialization/
210 Top 10 Big Data Companies in 2023: https://innovatureinc.com/top-10-big-data-companies/
211 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
212 European Data strategy: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en
213 European Data strategy: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en
214 Data Act: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113
215 Ibid
216 Data Governance Act: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

- **GDPR**[217]: enforces the data processing requirements rooted in 7 general principles for privacy, with the purpose to handle personal data in a proper, ethical and legally compliant way.

2.4 Intelligence

The next layer is the intelligence layer, which involves the artificial intelligence algorithms that operate on data. There is a strong linkage between this layer and the previous layers. Advanced deep learning algorithms for example require GPUs, graphic processing units. These were originally developed for the gaming industry.[218] The American company Nvidia is an important developer of such chips. Intel is also an important maker of chips for artificial intelligence.[219] There is a whole variety of specialized chips like tensor processing units (TPUs) for advanced AI and large US technology companies such as Microsoft and Google make these themselves.[220] Moreover, this intelligence layer is strongly connected with the cloud layer, which is why the providers of cloud services such as Amazon and Microsoft also provide AI services in combination with cloud services.[221]

R&D

When looking at intelligence from the R&D perspective the US and China are leading. Both have highly advanced capacities to develop algorithms and large data sets to train these algorithms on.[222] However, China has an edge over the US.[223] This relates to the availability of data to develop specific AI applications. According to Lee, AI has entered an application phase in which the emphasis will be less on fundamental science than on the availability of data for specific applications.[224] China has an edge because of the size of the Chinese population and the high percentage of global data that is produced inside the country.[225] Moreover, due to less strict privacy regulation in China compared to the EU, much of this data is relatively easily accessible for AI developers. In terms of the fundamental science of algorithm development, China still lags the US, but it is rapidly catching up.[226] Chinese scientists and organizations are increasing their share in global citations and patents.[227]

When focusing on the **future developments** of quantum computing there are new requirements for this technology layer; Since quantum computing relies on an inherently different structure of the underlying (quantum) bits compared to existing computers, there is a need for a completely new branch of algorithms to solve computational problems that are (re)designed to be solved on a quantum computer. These are referred to as quantum algorithms and open the doors to solve problems in the field simulation, optimization and AI in completely new, and sometimes improved, ways[228, 229].

Furthermore, the most important application of quantum algorithms related to national security is the ability to break existing encryption protocols by allowing for an exponentially faster algorithm to solve the underlying complex

217 Understanding the data protection principles in the GDPR: https://www.cyberpilot.io/cyberpilot-blog/data-protection-principles-the-7-principles-of-gdpr-explained/#:~:text=Short%20Summary%3A,Integrity%20and%20Confidentiality%3B%20and%20Accountability.
218 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
219 Ibid
220 Ibid
221 Ibid
222 Ibid
223 Ibid
224 Ibid
225 Ibid
226 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
227 Ding, J. (2018). Deciphering China's AI Dream: The context, components, capabilities, and consequences of China's strategy to lead the world in AI. Future of Humanity Institute, Oxford
228 Quantum algorithms: an overview | npj Quantum Information (nature.com)
229 Quantum machine learning | Nature

mathematical problem[230]. This is a key driver for governments to take part in the "space-race" towards building a large-scale quantum computing system that is able to effectively perform this task. Defensive measures against this threat can already be taken, either by upgrading the underlying mathematical problem (also referred to as post-quantum or quantum-resistant cryptography), or by employing quantum encryption keys through quantum communication networks. However, these require developing new mathematical models, protocols and partially hardware infrastructure, so in general new forms of intelligence.

Commercialization

When looking at the intelligence layer from the commercial perspective fields of AI such as speech recognition and machine vision, China has leading companies such as iFlyTek, SenseTime, and Hikvision.[231] iFlyTek, one of the speech recognition company has for instance 700 million users, twice the amount of people that use Apple's Siri.[232] China's large technology companies, Baidu, Alibaba, Tencent are integrated platforms that combine all kinds of data which also makes them leading in AI.[233] Jefrey Ding made an estimation of global AI capacities. In contrast with Lee, he argues that the US has an edge over China. This is based on the lead in fundamental science, but the largest advantage he mentions is the semiconductor hardware.[234] China is still heavily reliant on advanced chips produced by American companies.[235]

As mentioned in the section about data (see section 2.3) EU's position in data is weaker than both China and the US. Furthermore, the EU does not have leading technology companies in this domain such as in the US and China.[236] There are specific European companies that have AI in the core of their operations like Spotify and Booking.com. But these are more specialized niche players and are reliant on US capital.[237]

A leading player in the field of commercializing quantum and AI algorithms is the Alphabet spin-off SandboxAQ, which raised $500 million (€450 million) in initial funding.[238] The spin-off is aggressively setting up partnerships with leading public and private institutes globally to develop and commercialize quantum technology, including quantum algorithms, and in particular in relation to AI.[239]

Policy and regulation

The national and EU-wide AI strategies show increased momentum, but the scale of ambitions and investments are still far below those of the Chinese and American AI strategies.[240] Meaning that there is a lack of digital sovereignty on this layer.

However, the European Commission took several measures and announced for instance in January 2024 that, following the political agreement reached in 2023 on the EU AI Act they intend to proceed with a package of measures (the AI Innovation Strategy) to support AI startups and SMEs in the EU.[241] Alongside these measures, they also announced the creation of the European AI Office which will start in February 2024.[242]

230 Algorithms for quantum computation: discrete logarithms and factoring | IEEE Conference Publication | IEEE Xplore
231 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
232 Ibid
233 Ibid
234 Ibid
235 Ibid
236 Ibid
237 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
238 AI And Quantum Computing Startup SandboxAQ Snags $500M (crunchbase.com)
239 SandboxAQ Collaborates with More Than 30 Universities, Corporations & Educational Organizations to Expand AI & Quantum Training (thequantuminsider.com)
240 SandboxAQ Collaborates with More Than 30 Universities, Corporations & Educational Organizations to Expand AI & Quantum Training (thequantuminsider.com)
241 European Commission Announces New Package of AI Measures: https://www.insideprivacy.com/artificial-intelligence/european-commission-announces-new-package-of-ai-measures/
242 Ibid

The European Commission intends for the AI Innovation Strategy to help the EU "fulfil its potential of becoming a global frontrunner in trustworthy advanced AI models, systems and applications". Therefore the European Commission has committed to delivering the following measures[243]:

- Create "AI Factories" across the EU, which will bring together supercomputing infrastructure and human resources to further develop AI models and applications.
- Make data spaces available through the development of "Common European Data Spaces", with the goal of improving the availability of and access to high-quality data for start-ups and innovation communities to train their AI systems, models and applications. (For more details on data spaces see the section about data sharing infrastructures).
- Support the development of novel use cases in a number of industrial sectors including robotics, health, and manufacturing with the "GenAI4EU" initiative.
- The AI Innovation Strategy includes an overall public and private investment package of around €4 billion through 2027 dedicated to generative AI.

The AI Office is a centralized EU agency within the European Commission that will support the implementation and enforcement of the AI Act in collaboration with the European Commission and EU Member States' national competent authorities. Specifically, the AI Office's mandate is to[244]:

- Ensure the uniform implementation and enforcement of the AI Act,
- Support and monitor the development of AI markets and policies across the EU,
- Develop and coordinate collaboration and cooperation initiatives within and outside the EU.

2.5 Applications

The next layer is the application layer. The previous layers are not focusing on the customers and the application areas such as the various sectors. Here, all previous layers are combined and used to create specific digital applications and services in various domains.[245] This can involve diverse services like social media networks, chat apps, search engines, healthcare applications, applications in the manufacturing domain, mobility domain etc.

The application layer is too diffuse to have a coherent discussion on the R&D perspective, commercialization perspective and policy perspective. Therefore this layer will be approached from the more generic global perspective. Given the high dependence of the previous digital technology layers on a limited number of non- European countries and organisations, it is no surprise that this dependence is extended to the application layer.[246]

However, there are also areas in which Europe and the Netherlands are still strong. Europe and the Netherlands are for instance strong in complex equipment which require high precision manufacturing.[247] The market for such products will expand when moving into the digital anything – everywhere domain. Examples include e.g. healthcare, manufacturing equipment, the built environment and mobility. As the equipment becomes much more digital, Europe and the Netherlands have the potential to lead on this layer.[248]

2.6 User Interfaces

The next layer is the user interfaces layer. Human beings use language and semantics a computer cannot understand, that means that to 'communicate' with a digital system, we need to translate human language into computer language.[249] The interface is the layer that manages this translation process. The Graphical User Interface (GUI) of the mobile phone for instance has replaced desktop screens, mouses and T9 keyboard as the dominant

243 European Commission Announces New Package of AI Measures: https://www.insideprivacy.com/artificial-intelligence/european-commission-announces-new-package-of-ai-measures/
244 Ibid
245 European Digital Sovereignty a Layered approach: European Digital Sovereignty: A Layered Approach | SpringerLink
246 Stolwijk, Punter et al. (2022), Bridging the Dutch and European Digital Sovereignty gap: https://publications.tno.nl/publication/34639349/urAkBu/TNO-2022-R10507.pdf
247 Ibid
248 Ibid
249 Freedom lab Introduction to the stack https://www.freedomlab.com/posts/an-introduction-to-the-stack

interface.[250] However, users approach services through various types of user interfaces. This interaction may occur along all kinds of different modalities such as, for instance vision (screen, Virtual Reality headset), speech (voice assistant), gestures (3D cameras, haptic devices) and hearing (wireless earphones).[251] User interface play a dual role: On the one hand, they determine the information and experience that digital systems convey, and on the other hand they dictate the type of data that can be collected about the end user and their environment.[252] Other examples of user interfaces are[253]:

1. Virtual reality (VR) glasses: visually transport the user to an immersive virtual world through a stereoscopic first-person perspective. The convergence of high-quality yet affordable display technology.
2. Augmented Reality (AR) glasses: project virtual elements over the physical world. The ultimate blending of realities.
3. Voice-controlled interfaces: advances in Natural Language Processing (NLP), voice recognition and speech synthesis in combination with new hardware interfaces such as wireless earphones and smart home systems will further improve the quality of voice-controlled interfaces.
4. Hand tracking for control: using your own hands for controlling the experience, removing the need for controllers and making the experience more intuitive and immersive.

R&D

In recent times, the use of user interfaces such as of virtual reality (VR) have exploded as technology has advanced. In many ways, VR transforming how individuals interact with digital content. With ongoing research and development (R&D) in virtual reality taking place, VR start-ups are important property.[254] Apple is known for investing large amounts of money, time and resources into virtual reality and the company acquired many VR startups over the last 10 years.[255] Other important players are Meta (US) and Microsoft (US), Google (US), Samsung (Asia), Varjo (EU) and Magic Leap (US).[256] Relevant chipset manufacturers, are for instance Qualcomm (US) and Nvidia (US).[257] A relevant platform provider is for instance Unity (EU/US).[258]

Commercialization

Large tech companies such as Apple, Meta and HTC, have all invested in the advancement of virtual reality technology, with products such as Apple Vision Pro, Meta Quest 3, HTC Vive XR Elite., but also Finish company Varjo is active and developed Varjo XR-4. These companies play critical roles not only by providing the necessary hardware but also by funding and supporting software development.[259] Such large investments enable them to shape the direction of the industry and ensures a consistent level of quality and innovation. In contrast, smaller startups and individual developers often bring fresh ideas and unique perspectives, challenging the status quo and pushing the boundaries of what is possible within the VR space.[260] However, most companies concerned with developing virtual reality and metaverse technologies are domiciled outside the EU.[261]

Policy and regulation

Additionally, from the perspective of Policy and Regulation, various policy measures of the EU are implemented. Examining earlier examples of AR and VR, the European Commission has acknowledged

250 Freedom lab Introduction to the stack https://www.freedomlab.com/posts/an-introduction-to-the-stack
251 Ibid
252 Ibid
253 Outlook Digitalisation 2030: link
254 R&D In The Virtual Reality Industry | ForrestBrown
255 Based on expert input
256 Ibid
257 Based on expert input.
258 Ibid
259 Ibid
260 Who Develops Virtual Reality? Key Players And Innovators In The Industry - Draw & Code (drawandcode.com)
261 EU lawmakers want metaverse strategy that supports the bloc's businesses | The Block

the potential of the virtual worlds, also known as the metaverse (when referring to a network of interconnected virtual worlds). Recognizing both its opportunities and challenges, the European Commission has adopted a strategy on Web 4.0 and Metaverses to steer the technological transition and ensure an inclusive, secure, and innovative digital landscape for EU citizens, businesses, and public administrations.[262] However, alongside opportunities come challenges that must be solved, including the need for trustworthy information, digital skills, user acceptance, and fundamental rights. The European Digital Rights and Principles will guide a human-centric vision for virtual worlds, reflecting EU values.[263] Besides that the European Commission set out a plan to take the lead in the metaverse - shared virtual worlds accessible through the internet - and to prevent Big Tech dominating a nascent sphere that could boost economic growth.[264]

2.7 Smart Habitat

The next layer is the smart habitat layer, that points to our digitized environment. For example, the smartphone has become our wallet to pay and functions as our biometric passport to enter a restaurant during a pandemic.[265] Hence, our increasingly smart living environment forms an interface between society and the digital Stack that facilitates those services, provides us with information and derives data from us and the activities we execute.[266] This makes our living environment a source of data and because of digitalisation in various sectors and the addition of robotics, our environment itself is becoming more dynamic and responsive.[267] In addition, this smart environment may provide the permanent possibility of monitoring, surveillance and transparency, partly initiated by the need for coordination between all smart devices and connected people.[268] This could also lead to better protection and automation of energy, water and transport. However the downside is that a low digital sovereignty on the aforementioned technical layers also leads to dependencies on Big Tech players on this layer. Smart cities has for instance a lot of US players involved such as Cisco, IBM, Microsoft and Intel, but there are in this case also some players from Europe such as Siemens and Schneider Electric[269] Or from Japan such as Hitachi.[270]

The fact that we enter into a Smart habitat also means a clear need for policy instruments that stimulates awareness creation and education to stimulate at one hand the digital skills of the citizens living in a digitized environment. On the other hand this also requires clear awareness creation on the opportunities (such as more efficiency, transparency, higher productivity etc.) and potential risks of digitalisation (such as cyberattacks, privacy problems and other problems that occur when being highly digitalized). More details on these instruments can be found in section 5.2.

2.8 Neo-Collectives

Digitalisation also creates new cultural practices and communities called neo-collectives.[271] This concerns both the virtual and physical realm. As digital technology has fundamentally changed the way we socialize, work, date, cook or shop. It has created new protest groups that originated on social media and developed vibrant internet communities such as those we see nowadays on TikTok. Due to the digitalisation of daily life, new political and cultural collectives are arising, while these neo-collectives in turn (re)shape the Stack in a social way.[272] That is why this layer is part of the stack.

Like with the previous layer we also see here that the dependence on Big Tech on the technical layers has an impact on this

262 From Virtual to Reality: The European Commission's Strategy for Web 4.0 and Metaverses | Digital Future Society
263 Ibid
264 EU looks to take lead in metaverse world, avoid Big Tech dominance | Reuters
265 Freedom lab Introduction to the stack https://www.freedomlab.com/posts/an-introduction-to-the-stack
266 Ibid
267 Freedom lab Introduction to the stack https://www.freedomlab.com/posts/an-introduction-to-the-stack
268 Outlook Digitalisation 2030: link
269 Top companies in the Smart Cities Market: link
270 Ibid
271 Freedom lab Introduction to the stack https://www.freedomlab.com/posts/an-introduction-to-the-stack
272 Ibid

layer. Because via platforms such as TikTok and Facebook new communities are highly influenced based on fake news practices and other anti-social practices that have sowed societal discord and conflict in many jurisdictions.[273] These platforms often originate as a communication tool to facilitate social interactions between individuals through the internet[274] and have evolved into complex ecosystems of digital interactions between a diverse range of stakeholders, including advertisers, digital entertainment service providers, and anyone seeking to connect with individual social media account holders.[275]

2.9 Neo-Governance

Digital technology results a fundamental shifts in many sectors and in society at large. Digitalization can therefor require new forms of governance and changes in existing governance forms. This is called the neo-governance layer[276] and concerns:

- How governments change their policy around the adoption of digital technologies: (e.g. the Netherlands actively promoting open source software adoption within its government and public administration).[277]
- New institutional structures and forms of governance arising from the digitalization[278] such as Public-Private Partnerships (PPPs) that function as an enabler to mobilise the digital transition. At the same time digital technologies and solutions can streamline the PPP project cycle and enhance the speed and integrity of the PPP projects.[279] An example of a PPP is the EU-US Trade and Technology Council[280], in which the EU and the US are partners strongly committed to driving digital transformation on new technologies based on their shared democratic values, including respect for human rights.[281]
- The impact of digitalization on existing institutional structures such as the World Trade Organization. The WTO is committed to achieve a rules-based international trading system.[282] However, the WTO has to deal with weakening global governance structures, geopolitical disputes and changing global realities.[283] The lack of boundaries in the digital space contributes to these geopolitical disputes, as data and technology are weaponized across borders, and hacking of critical infrastructure happen more frequently.[284] To keep pace with such developments in the rapidly changing trading environment, many members, including the EU, believe that the WTO needs fundamental reform.[285]
- New players interfering with existing governance structures such as private players in the military domain that can have unwanted effects. An example is the role of Elon Musk in the war between Ukraine and Russia. In 2022, the American CEO refused to activate the Starlink telecommunications satellite network, operated by his

273 Ibid
274 Digital Dominance and Social Media Platforms: Are Competition Authorities Up to the Task? https://link.springer.com/article/10.1007/s40319-023-01302-1
275 Armental M (2020) Facebook launches shopping platform. Wall Street J. At https://www.wsj.com/articles/facebook-launches-shopping-platform-for-small-businesses-11589919007. Last visited 28 Nov 2021
276 Freedom lab Introduction to the stack https://www.freedomlab.com/posts/an-introduction-to-the-stack
277 Updated report on the state of open source in the Netherlands. https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/updated-report-state-open-source-netherlands
278 The stack: https://www.freedomlab.com/frameworks/the-stack
279 Ibid
280 EU-US Trade and Technology Council: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en
281 EU-US Trade and Technology Council: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en
282 De Europese Unie en de Wereldhandelsorganisatie: https://www.europarl.europa.eu/factsheets/nl/sheet/161/de-europese-unie-en-de-wereldhandelsorganisatie
283 Reviving the WTO and rules-based trading: The EU's role: https://www.ceps.eu/ceps-publications/reviving-the-wto-and-rules-based-trading/
284 Geopolitics of the Digital Economy: Implications for States and Firms: https://insights.aib.world/article/67966-geopolitics-of-the-digital-economy-implications-for-states-and-firms
285 https://www.europarl.europa.eu/factsheets/nl/sheet/161/de-europese-unie-en-de-wereldhandelsorganisatie

company SpaceX, over areas close to the Crimean peninsula, occupied by Russia since 2014.[286] Kyiv has said that the recapture of this area is one of its war goals.[287] By doing so, the CEO prevented a Ukrainian drone attack on Russian warships of the Black Sea Fleet at the Sevastopol naval base.[288]

To stimulate the positive impact on this layer and mitigate the negative impact of digitalization Research Institutes can fulfil an important and independent role. For instance by giving advice on the development of new institutional structures based on their technological, legal and ethical expertise. But also by orchestrating the aforementioned PPPs.

286 Elon Musk, an unpredictable partner in the defense area: https://www.lemonde.fr/en/international/article/2023/09/10/elon-musk-an-unpredictable-partner-in-the-area-of-defense_6131377_4.html
287 Ibid
288 Ibid

3. Scenario's for digital sovereignty

The digital technologies from the stack described in Chapter 2 can be mapped to scenario's related to digital sovereignty to provide a clear overview on:

1. The level of digital sovereignty for all digital technologies.
2. The feasibility of Europe and the Netherlands to act.

These four scenarios are developed in a former investigation[289] and are based on two related drivers that are relevant to act on global level[290]:

- The first driver concerns international cooperation among foreign partners, which can be strong or weak. Strong cooperation is based on frequent reciprocity among foreign companies, and complementarity and interoperability among their digital technologies. Weak cooperation is characterised by very limited or no reciprocity among foreign companies, and lack of complementarity and interoperability among their digital technologies.
- The second driver is economic globalisation (or 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 companies can execute trade activities without restrictions (e.g. without high import duties) the ease of trade among foreign companies 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 6[291]).[292]

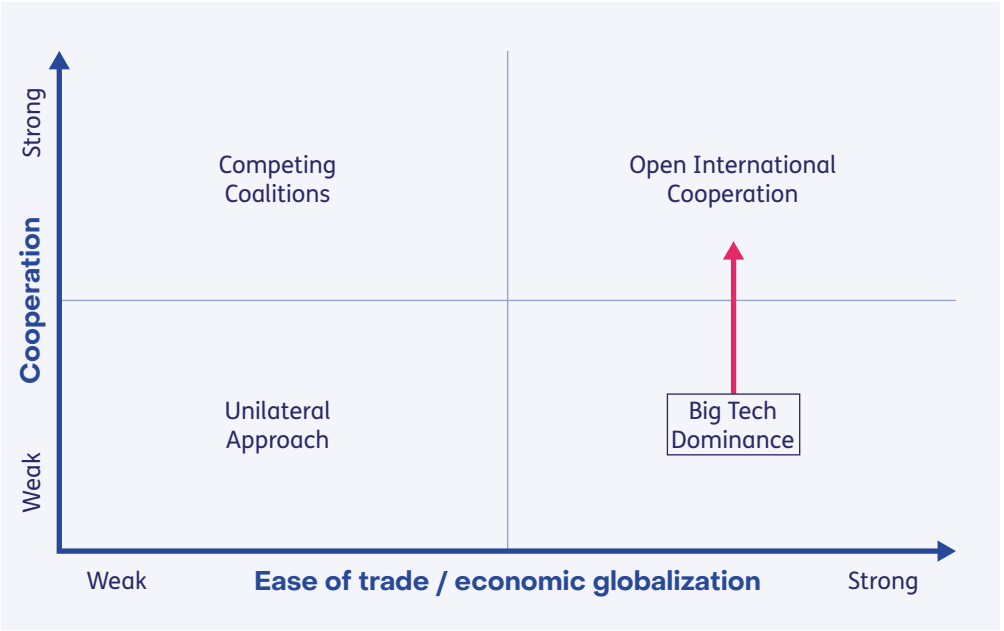

Figure 6 *Four scenario's related to digital sovereignty*

In the next sections (3.1-3.4) each of these scenarios are described followed by the mapping of the technologies[293] per scenario in section 3.5. In section 3.6 we discuss how the technology mapping looks like per scenario if no measures are taken. In section 3.7 we discuss how the technology mapping looks like per scenario if measures are taken. These mappings are based on expert views.

289 Stolwijk, Punter et al. (2022), Bridging the Dutch and European Digital Sovereignty gap: https://publications.tno.nl/publication/34639349/urAkBu/TNO-2022-R10507.pdf
290 Ibid
291 Partially based on: https://www.weforum.org/agenda/2019/01/four-future-scenarios-for-trade-and-investment-which-one-will-win/
292 Partially based on: https://www.weforum.org/agenda/2019/01/four-future-scenarios-for-trade-and-investment-which-one-will-win/
293 These technologies also include the Data layer

3.1 Scenario 1 Open international cooperation

Scenario 1 is Open international cooperation, which may be seen as the preferred scenario since this scenario appears to provide the best chances for a level of digital sovereignty that preserves Europe's societal values at one hand and the social market economy on the other hand (e.g. in terms of international cooperation and trade). In this scenario[294], foreign companies come together to cooperate based on complementary digital technologies and interoperability, and trade flows move easily across country borders. Major economies jointly commit to address points of conflict and cooperate to revitalize the WTO through 'plurilateral' negotiations, with significant contributions from advanced and emerging economies. On global level actions are taken on major issues such as: modernizing trade rules; minimizing distortions created by unfair subsidies; governing digital trade; strengthening the WTO's monitoring and dispute settlement functions. Public and private stakeholders 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 as well as productivity gains. In this scenario Europe and the Netherlands are substantially investing in the digital infrastructure and they are leading in setting standards. We should, however, not be naïve about the potential risks and downsides of this scenario. It can degenerate into neo-liberalism which has turned out to fail in delivering fair and equitable economic and social progress. If kept unchecked, such a scenario may fail to safeguard democracy and instead incite another wave of populism and protectionism.[295]

3.2 Scenario 2 Competing coalitions

Scenario 2, is the Competing coalitions[296] scenario, foreign companies cooperate in this scenario, 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 impact national security. Amidst these differences, trade and investment flows are directed by political intervention next to price signals, and pressure comes to bear on multinationals to restructure and localize value chains. It becomes harder to make progress within the WTO and multilateral governance gets limited to regional blocs. Heightened concerns over the geopolitical and security implications of investment result in the bifurcation of investment flows (e.g. China versus the US together with the EU). Some regions and global businesses become caught in between different spheres of influence. In a zero-sum dynamic, individual countries come under pressure to lean towards one bloc over another. In chapter 4 this corresponds to pursuing digital sovereignty through partnerships of likeminded countries. Geopolitical dynamics will likely result in a competition between US and China, with Europe's position being less clear. Military conflict may force Europe to choose sides. It is assumed but not proven that this has negative repercussions for geopolitical stability and economic development. Likely, Europe will remain for years highly dependent in the digital domain on the US. Even if this is less optimal for digital sovereignty than scenario 1, it is also less worse than scenarios 3 and 4.

3.3 Scenario 3 Big Tech dominance

Scenario 3 is the Big Tech dominance scenario.[297] This is the scenario in which most digital technologies are controlled by foreign non-European companies who act unilaterally rather than cooperatively. Innovation of digital technologies races ahead of regulation. There is limited interoperability and technological complementarity hindering a cooperative approach among foreign companies. 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 global business or economic globalization and a high level of easiness of trade for large non-European Big Tech firms that are based on 'hyperscaler' based business models. Small and medium sized enterprises, however, become in an unfortunate position by high barriers to entry in some digital 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 enhances even more

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

295 Dani Rodrik, a famous international political economist, argues that a trilemma exists between (hyper)globalization, sovereignty, and democracy, meaning: "you can have two, not three". In this scenario, if unbalanced, it is likely democracy that loses out.

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

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

(the always-present) incentives for theft and other forms of economic espionage. Fragmented regulatory frameworks for data flow governance raise cybersecurity risks and increase costs. Small businesses and consumers in weaker economies might lose access to the latest digital technologies and services. Consumer and worker interests become dependent on the Big corporates, who can move jobs around. Democracy will suffer and both individual and state sovereignty based on democracy will increasingly be sidelined by 'corporate sovereignty'. 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 especially on regulation.

3.4 Scenario 4 Unilateral approach

Scenario 4, the Unilateral approach[298], 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, resulting in even stronger de-globalization than in scenario 2. The global economy slides into protracted decline, creating major domestic challenges for most countries and foreign companies. These challenges include higher costs for consumers and rising unemployment, as well as 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.

3.5 Mapping according to the current status

There is actually no technology that fully fits the **Open International Cooperation scenario.** (Micro)chips, Satellites and Edge infrastructure are currently positioned at the borders of this scenario. As mentioned in Chapter 2 both the US and Asia are fulfilling a strong role in the (micro) chip area. The EU's share in the chips industry has been declining, but it is still a considerable producer of chips. Besides that we see competition and cooperation among the US, Asia and Europe in the semicon supply chain. Therefore (micro) chips are positioned between the Open International Cooperation scenario and the Competing Coalitions scenario. Satellites are currently dominated by the US. But Europe is also active to have IRIS2, the European Starlink, operational by 2027. As IRIS2 provides chances for a more open international cooperation this technology is mapped between the Open International Cooperation scenario and the Big Tech Dominance scenario. Edge Infrastructures are also mapped on the border between Open International Cooperation scenario and the Big Tech Dominance scenario. This technology is mapped on this border as Edge Infrastructure is in the hands of Big Tech, but it is still in its early stages and especially Germany is focusing on this technology in the manufacturing domain, which still provides new opportunities for Europe.

Telecom (mobile networks) is the only technology that fully fits the **Competing Coalitions scenario.** Competing coalitions are for this technology Huawei, Nokia and Ericsson. (Micro)chips and Intelligence are positioned on the borders of this scenario as well. The mapping of the (Micro)chips on this border is already discussed under the Open International Cooperation scenario. The reason why Intelligence is positioned on the border between the Competing Coalitions and the Unilateral approach is because for this technology we see competing coalitions between the US and China, but we also observe how China is getting stronger, which might lead to a real trade wars at the expense of cooperation.

Currently many technologies can be mapped to the **Big Tech Dominance scenario** such as: Data Sharing infrastructures (dominated by hyperscalers), Cloud infrastructures (dominated by hyperscalers such as Amazon, Google), Internet Cables (Microsoft, Meta, Amazon and Alphabet are becoming the largest shareholders). Edge Infrastructure and Satellites are positioned on the border of this scenario and the Open International Cooperation scenario,

298 Ibid

because these are technologies provided by Big Tech, but Europe also has some initiatives that could provide opportunities towards the Open International Cooperation scenario if the European initiatives in this area become successful (e.g. IRIS2, the European Starlink initiative for sattelites, the German activities on Edge Computing for edge infrastructures).

Data is as far as localization requirements are imposed either for national security or for lack of GDPR compliance of the data operator mapped to the **Unilateral approach.** The rationale behind this is that the EU's position in data is weaker than both China and the US. Besides that most data is in the silos from large Big Tech companies, which means data is also related to the Big Tech scenario.

For an overview of each of the digital technologies from the stack model per scenario see Figure 7.

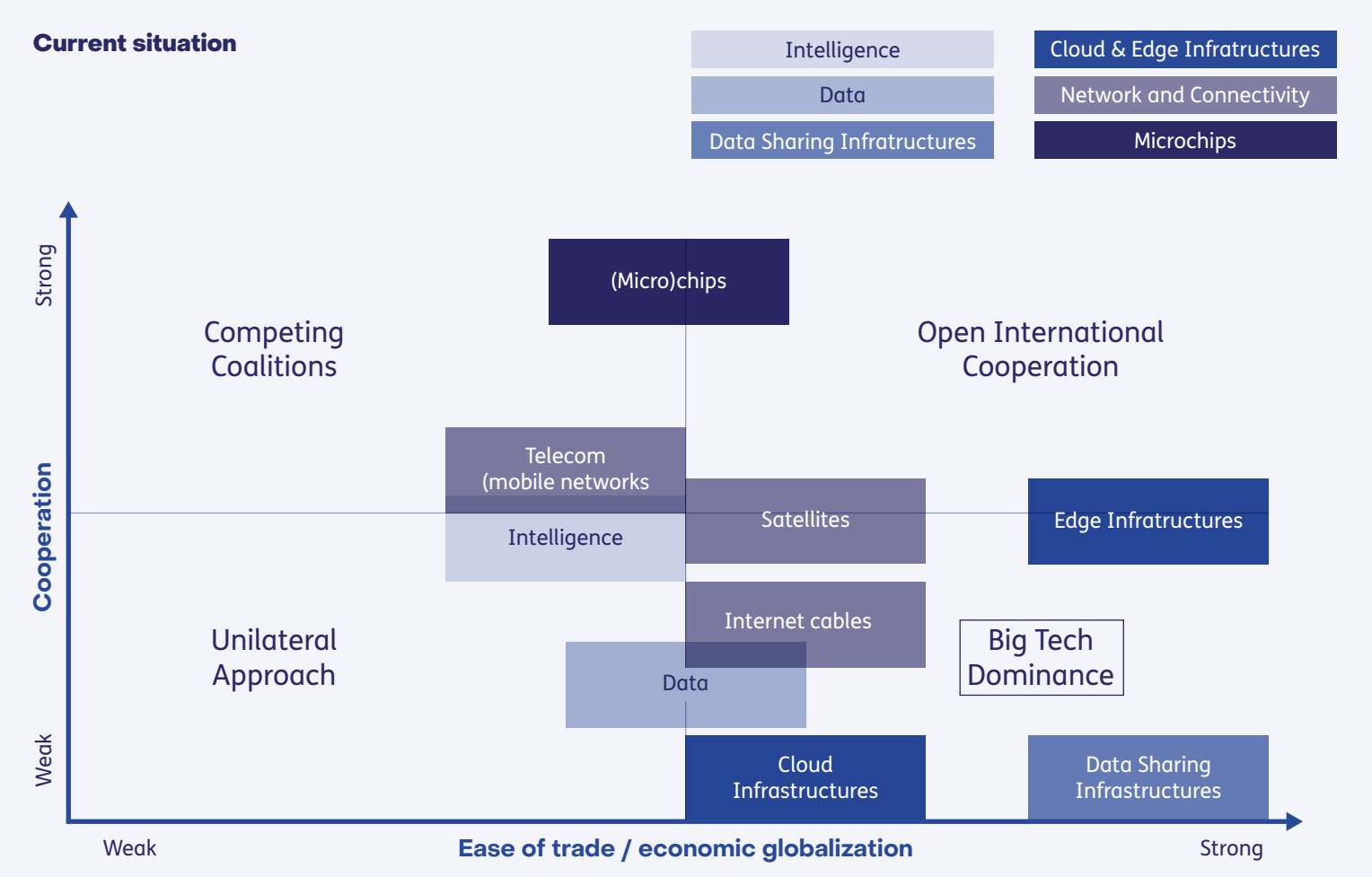

Figure 7 *Mapping of digital technologies coming from the stack model per digital sovereignty scenario*

3.6 Mapping with no policy measures

If no measures are taken experts expect that the situation gets worse, meaning that the following technologies will probably move towards the following scenario's[299] (see Figure 8):

- (Micro)chips are expected to move to the Competing Coalitions scenario; if Europe's role in the Chip Industry might further decline Europe will lose the strong competition among the US and Asia.
- Telecom (mobile networks) is expected to move to the Big Tech Dominance scenario in which Huawei becomes the winner who takes it all. Thanks to the ban of the company by various countries this did not happen yet.
- Edge infrastructures are expected to move to the Big Tech dominance scenario if this technology will be pushed further by the hyperscalers, who already have an important role in this area.
- Data will probably move to the Big Tech Dominance scenario given the fact that much of the data is stored in the silos of Big Tech companies.
- Intelligence will move towards the Big Tech dominance scenario as it is likely that the American hyperscalers will win this battle if no additional measures are taken.

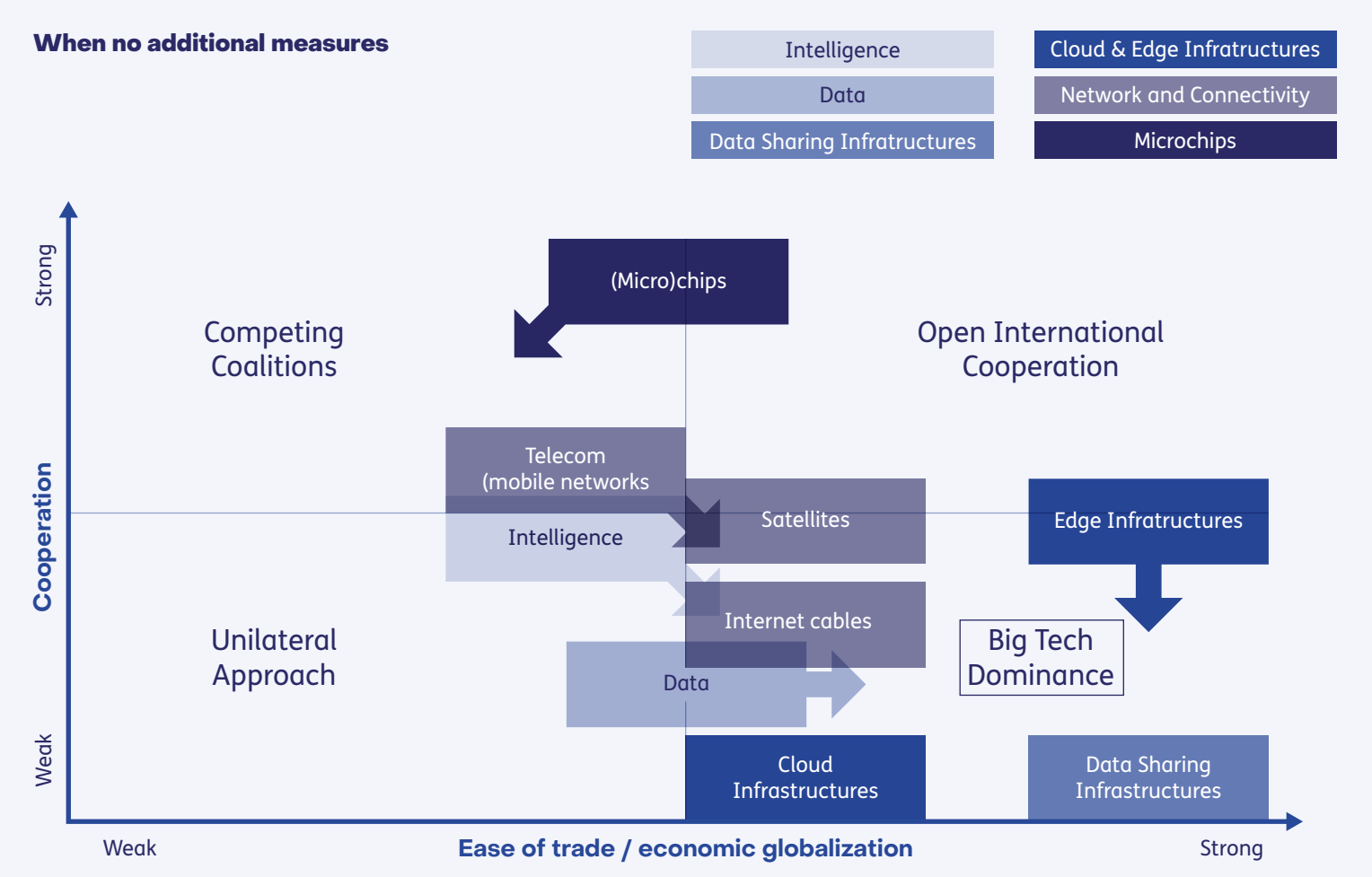

Figure 8 *Potential position of the technologies per scenario in case no additional measures are taken*

299 Based on expert discussions

When no additional measures are taken the following technologies are expected to keep the same position in the scenario model: Data sharing infrastructures, Cloud infrastructures, Satellites and Internet cables.

3.7 Mapping based on the ambition

In Figure 9 the ambition is presented on how the technologies should preferably be positioned related to the various scenario's on the mid to long term. This ambition is developed based on discussions with experts who indicated what the ambition should be when applying additional measures. It also takes in to account the realism of recognizing the dominance of foreign cloud providers. In this section we explain how the ambition looks like, starting with the most ambitious changes:

- The Data Sharing Infrastructures and Edge Infrastructures moves from the Big Tech dominance towards the Open International Cooperation scenario by further building on current European initiatives such as the Data Space initiatives, Gaia-X, IDSA for the Data Sharing Infrastructures and the German initiatives in the manufacturing domain focusing on the Edge Infrastructure.
- Cloud Infrastructures move a bit from the Big Tech Dominance scenario towards the Open International cooperation, based on the IPCEI CIS initiative and all the regulation that has

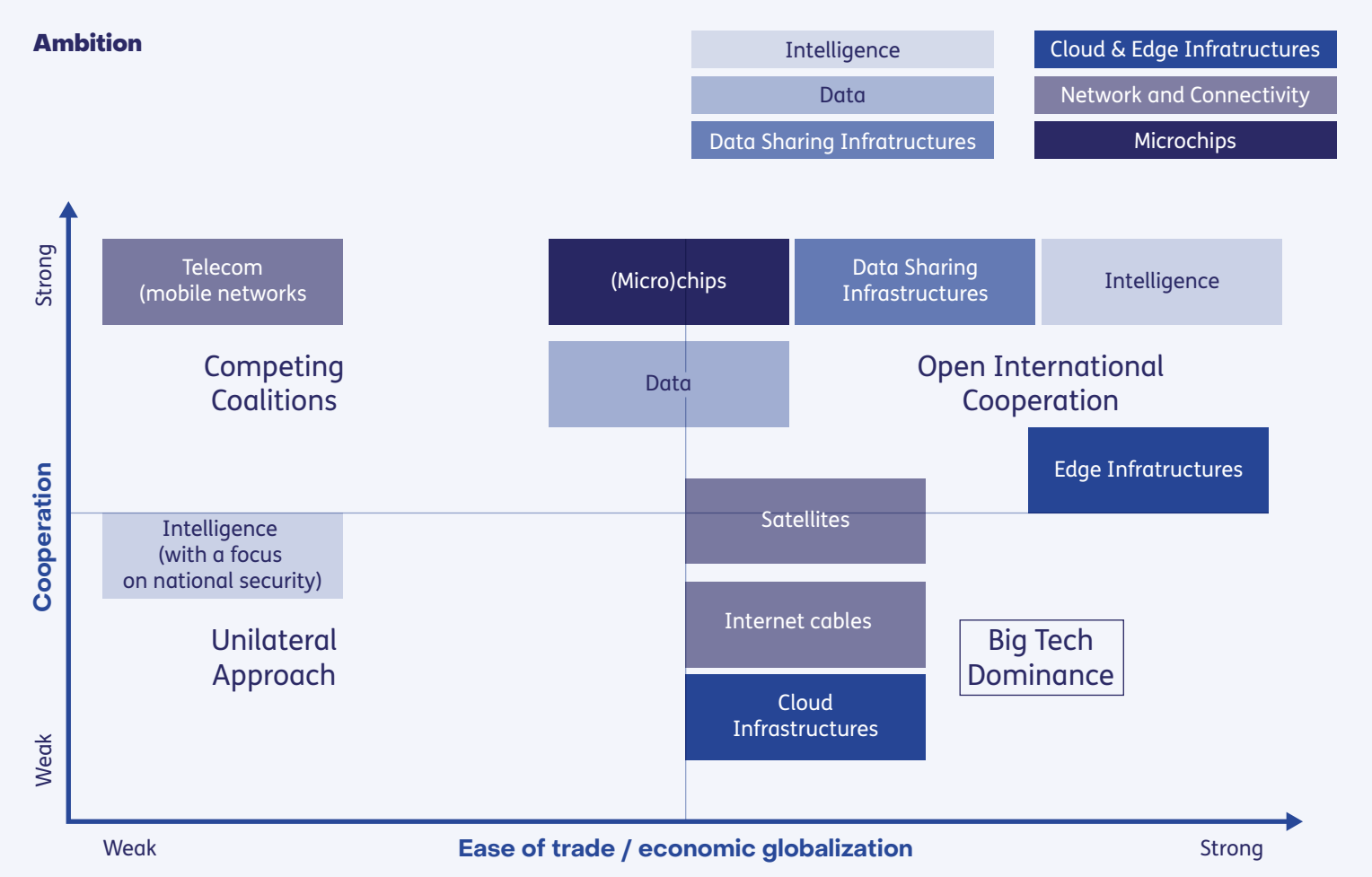

Figure 9 *Ambition of the technologies per scenario based on expert views*

been developed to regulate the Cloud infrastructure.
- (Micro)chips stays between the Open International Cooperation Scenario and the Competing Coalitions scenario by keepings ASML's strong position in producing chip manufacturing machines and by ensuring that the EU remains a considerable producer of chips.
- Telecom (mobile networks) stays in the Competing Coalitions scenario by ensuring that the European players Nokia and Ericsson remain among the competing coalitions. But it will move to the upper left of this scenario.
- Intelligence splits in a part that will move to Open International Cooperation based on common interest and a part that will move to the Unilateral Approach scenario for national security. This needs to be done by avoiding that Big Tech will determine the rules based on their recent developments in AI. Regulation (e.g. AI Act), standards and investment in R&D and public procurement play and important role here.
- Data would move from the border between the Big Tech Dominance scenario and the Unilateral Approach Scenario towards the Open International Cooperation, because there is a lot of global common interest in data from logistics to environmental and health, which needs to be further stimulated.
- To keep the Satellites between the Big Tech dominance scenario and the Open International Cooperation scenario it is important to build on the European IRIS2 satellite initiative for internet and communication.
- Internet cables are expected to stay in the Big Tech Dominance scenario given the fact that American players such as Microsoft and Amazon are important shareholders and given the prioritization for measures on other technologies by the experts involved in developing the ambition.

However, current measures are not sufficient according to the experts to realize the ambition. Therefore additional measures are described in Chapter 5.

4. Different perspectives on digital sovereignty

In this Chapter we discuss the impact of the current level of digital sovereignty seen from three different perspectives:

1 The Social Economic perspective
2 The Company perspective
3 The Cyber security perspective

4.1 Social, economic perspective

In this section the societal and economic impact of the lack of digital sovereignty is discussed.

Societal impact

The increasing dependence on the digital infrastructure and digital technologies of a limited number of non-European market players, has a terrible societal impact, which can be summarized as follows[300]:

- **Harms to society:** Each day reveals new harms caused by Big Tech to public values[301] such as hate speech which goes viral, advertising companies overseeing and owning massive information ecosystems. But also private firms selling intrusion systems online, having similar capacities to intelligence agencies but with limited democratic and legal oversight.
- **Influencing democratic values:** Social media platforms increasingly determine the rules of the game of our democracy. It is difficult for them to provide sufficient measures to counter dis-and misinformation, fake news and unwanted political influence (e.g. during elections) on their platforms. At the same time such matters are challenged as being a limitation of free speech.[302]
- **Controlling other countries:** A strong dependency on non-European high tech giants brings control of other countries, which have different rules for espionage, privacy and issuance of data. This contributes to various issues such as algorithmic in-transparency, privacy breaches, illegal data transfer etc.[303]

Economic impact

The increasing dependence on the digital infrastructure and digital technologies of a limited number of non-European market players, has a negative economic impact[304]:

- **Questioned competitiveness:** 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.[305]
- **Merger and acquisitions resulting in lack of competition:** However, when new potential competitors arise, Big Tech companies have the tendency to acquire those (European) start-ups that challenge them in their market.[306] 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.[307]
- **Economic sectors becoming dependent of Big Tech:** It also means a growing number of economic sectors that are becoming increasingly and

300 Stolwijk, Punter et al. (2022), Bridging the Dutch and European Digital Sovereignty gap: https://publications.tno.nl/publication/34639349/urAkBu/TNO-2022-R10507.pdf
301 Weakened democracy is another harm caused by Big Tech. https://www.ft.com/content/9adb3a15-d610-4bd6-bae0-a87dc4f315c6
302 CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'. https://userfiles.mailswitch.nl/files/3443-acde5625f3ee1664315ae1ef6132a594.pdf
303 Ibid
304 Stolwijk, Punter et al. (2022), Bridging the Dutch and European Digital Sovereignty gap: https://publications.tno.nl/publication/34639349/urAkBu/TNO-2022-R10507.pdf
305 DGAP 2021. Europe's capacity to act in the Global Tech Race. P. 23
306 Big tech dominance (2) : a barrier to technological innovation ? - Fondapol
307 Towards a European digital sovereignty policy. https://www.lecese.fr/sites/default/files/travaux_multilingue/2019_07_souverainete_europeenne_numerique_GB_reduit.pdf#page8

quickly dependent on foreign high tech companies and dominant platforms.[308]

- **Non-EU companies enter critical infrastructures:** Potentially, it also means that the non-EU companies enter critical infrastructure markets such as data centres.[309]
- **Stimulating tax avoidance:** Furthermore, the dominant position held by the main digital platforms has favoured the implementation of complex tax optimisation and tax avoidance frameworks.[310]

4.2 Company and organisation perspective

It is important to also have the individual company and organisation perspective on digital sovereignty, which will be covered in this section. Therefore we cooperated with CIONET to interview more than 20 CIOs from various organisations (e.g. organisations supplying energy) and companies (e.g. food companies, companies selling clothing) about their perspective on digital sovereignty.

State of play

The CIOs involved in this research view digital sovereignty most often from the data sovereignty perspective.[311] In many cases they take the perspective of control over the infrastructure.[312] In some cases they take the perspective of strategic autonomy from vendors.[313] We expected that resilience (cybersecurity, business continuity, etc.) would be the main driver. However, the CIOs indicated that the added value of data sharing is actually the key driver for them. Risk management remains important. This was particularly mentioned by public organisations and organisations in the financial domain. It was especially important for organisations that are working on critical physical infrastructures (such as ports, utilities, the energy sector etc.). Although all CIOs indicated digital sovereignty is of high importance for the current and future digital strategy, the topic as such is for most organisations not yet an explicit part of their current roadmaps.[314]

Key findings

Key findings from discussions with the CIOs are[315]:

- **Their strategy for digital sovereignty is driven by the added-value of data:** When the organisations involved in the investigation have a digital sovereignty strategy, it is mainly driven by the added-value to the organisation.
- **Cloud technologies of hyperscalers are commonplace for them:** Most CIOs indicated that they are already using cloud technologies for line-of-business applications. Most of them are using hyperscaler infrastructures to move their data to the cloud. This is in line with the trend that more and more data will be shared within and between these organisations and put in the cloud.
- **Technical and cost concerns are currently driving their cloud based digital infrastructures:** Both pragmatic technical and cost concerns are the main drivers of the current digital infrastructure set-up for companies. This is often still a hybrid cloud approach, meaning that part of the data is stored in the cloud and part of it resides on-premise or in private cloud environments. Many CIOs indicated that they expected this to evolve as more critical and sensitive data will be put in the cloud in the future.
- **There is a limited assessment of new European legislation on data:** Only a few CIOs indicated that they have already performed an explicit assessment of new European legislation (such as the Data Act, Data Governance Act, Digital Service Act). This is surprising as the impact can be similar to the introduction of GDPR, making it a compliance risk. In addition, new legislation on digital intermediaries and the mandatory provisioning of IoT-data can also provide new opportunities for the data economy as a whole and for individual companies.

308 https://www.lecese.fr/sites/default/files/travaux_multilingue/2019_07_souverainete_europeenne_numerique_GB_reduit.pdf
309 https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf
310 Ibid
311 Stolwijk, Punter, Hoekstra, (2023), Digital sovereignty: How Europe takes back control: https://publications.tno.nl/publication/34640695/aPvPww/TNO-2023-digital.pdf
312 Ibid
313 Ibid
314 Ibid
315 Stolwijk, Punter, Hoekstra, (2023), Digital sovereignty: How Europe takes back control: https://publications.tno.nl/publication/34640695/aPvPww/TNO-2023-digital.pdf

How digital sovereignty can impact the organizations and companies

We also discussed with the CIOs how digital sovereignty can impact their organisations and companies. The CIOs raised the following concerns related to the lack of digital sovereignty in Europe[316], of which the first two are strongly interlinked and have to do with the autonomy of the CIOs:

- **Concerns about the controllability of their digital landscape because:** The dependency on external infrastructures increases, data is shared between multiple stakeholders and at the same time data become more pervasive and critical to their business. This creates a more dynamic and complex situation for them, which can go beyond the current span of control of CIOs of individual organisations.
- **Lock-in effects of new digital infrastructures:** CIOs worry that it is easy to get access to a certain cloud platform, but expensive and difficult to get out and move data from one supplier to another. CIOs want to be able to make informed choices, facilitate transitions, migrations and maintain control when outsourcing their digital infrastructure and data sharing services.
- **Worries about business opportunities of alternatives for Big Tech:** Global business coverage of organisations - especially for multinationals - often requires global reach of digital technologies. This is currently limiting the market potential of smaller (European) cloud and data sharing offerings. Currently only larger providers of digital technologies, with a similar multinational reach, can provide the required level of service.
  - **CIOs regret there are no real European alternatives with a relevant scale yet:** Cloud solutions based on European initiatives, such as Gaia-X, need to find their way to the market. For many applications there is currently no viable European cloud offering. However, CIOs indicated that they are following these developments with interest and that this position could change in the future.
  - **Doing nothing about the current lack of digital sovereignty is not an option:** Some CIOs indicate that 'doing nothing' about the limited digital sovereignty is simply not an option as it will have a negative impact on:
    - The earning power of their organisations – today.
    - Their ability to stay innovative – affecting future earning power.
    - European norms and values, such as privacy. This is impacting corporate social responsibility in the digital realm.

4.3 Cybersecurity perspective

In this section the cyber security perspective is discussed based on18 interviews and desk research. After setting the scene, this section provides clear recommendations and better actions needed to strengthen the digital sovereignty for Europe and the Netherlands seen from the cyber security perspective.

Setting the scene

The need to increase digital sovereignty holds à fortiori for cybersecurity. Cyber-attacks that disrupt critical infrastructures (electricity, telecoms, hospitals) strike at the heart of economy and society. Cyber-theft of intellectual property and state secrets and dominance by foreign providers endangers the future of our companies and jobs. Foreign-sponsored disinformation undermines democracy.

Although cybersecurity *resilience* is being strengthened, cybersecurity *sovereignty* in the EU and the Netherlands is weak and getting weaker when governments and companies feel that they have little choice but to buy from foreign providers. Our digital infrastructures are increasingly controlled by non-European tech companies. There are hardly any Dutch cybersecurity companies with more than 250 employees. The cybersecurity market leaders in Europe are all foreign. Promising European cybersecurity companies with their talented staff are bought up by foreign investors with deep pockets.

Left unchecked, this will lead to a future with ever less control over the cybersecurity that is at the heart of our economy, society, democracy, and defence. The consequences are loss of talent, knowledge and home-grown companies and market share, and risk of foreign interference. Digital sovereignty in cybersecurity is about the very legitimacy of the EU and the Netherlands.

The following action-oriented recommendations are provided, based on an extensive study and expert interviews, to address improving cybersecurity sovereignty. The actions focus on increasing control, capabilities and capacities (3C) such that we can decide and act wherever cybersecurity is essential for our future economy, society, and democracy and defence.

316 Ibid

Recommendations

Cybersecurity sovereignty must become a top political priority in NL and EU. Research and Technology organizations and their partners should promote this in 2024 to the new NL government, which in turn should promote this to the new European Parliament and Commission in 2024-2025. Experts recognize that cyber-resilience may get strengthened but if fully based on foreign solutions this actually weakens autonomy. As a consequence home-grown cyber-security industry gets less opportunities and is marginalized, talent moves away, knowledge disappears, foreign dependency grows ever more. We are getting near to this situation today.

Realize full cybersecurity sovereignty with EU and politically-accepted international partnerships. Most interlocutors recommend: within 10 years. Cybersecurity sovereignty cannot be realized by the Netherlands and not even by the EU on their own. Partnering with politically-accepted likeminded countries, with long-term stability, will be necessary and may be even desirable for global stability. This is neither autarky nor protectionism but balanced economic and societal self-interest (that is, rather than the Unilateral Approach, this is a combination of Open International Cooperation and Competing Coalitions scenarios of Chapter 3).

Pursue joined-up policy actions as the only road to cybersecurity sovereignty. The Dutch government and her economic/societal partners should develop joined-up policy in existing cooperation and investment platforms and, as trailblazer, demand the EU to do likewise. Experts indicate that one cannot legislate oneself into sovereignty. Rather, joining up means being comprehensive, combining regulation with industrial, R&D, standardisation, investment, public procurement, education, trade, and international relations policies, all to build up and strengthening own capacity and capability, under own control.

Make the regulatory landscape for cybersecurity easier to navigate, in order to not lose time and effort with the risk that long-term autonomy erodes. All experts are very worried that the many cybersecurity regulations and initiatives are highly confusing leading to uncertainty, investment fear and huge workload. One action can be to provide European Commission Recommendations for cybersecurity in the EU Single Market based on an expert group reporting to the European Commission and the NIS Coordination Group and a workplan based on public consultation. The first Recommendation could be delivered within one year. Also, to be explored is a program of AI for the Cybersecurity Single Market.

Prioritize in relation to the severity of cybersecurity risks for sovereignty. The cybersecurity 'risk-space' is vast. Some risks are more severe and/or likely than others. Not everything can be tackled at once. The first priority is cybersecurity for the most critical risks, in the upper-right corner in Figure 10 (sovereignty for core of government, public administrations, cloud). Doing so cuts across the stack and delivers reusable solutions for the lower risk levels. Action plans should build on ongoing initiatives (cf., Kamerbrief on open strategic autonomy).

Define targeted policy actions and priority technological areas to tackle lacuna and build on national/EU strengths in technology and business models ('verdienmodel') such as in cryptography, threat intelligence, or services. Market regulation is largely in place, but significant gaps persist in risk capital, talent, demand-supply linkage (including for public procurement), and international industrial engagement. Fast wins include:

- **a** building a private-public partnership for scale-up investment in cybersecurity sovereignty
- **b** sovereign-by-default government procurement of cybersecurity with 'comply-and-explain'
- **c** specification/procurement of cybersecurity sovereign innovation in military-civil partnerships
- **d** skills and talent mobility support notably towards East European and likeminded countries
- **e** join up economic affairs and foreign policies (NL) and internal and external policies (EU).

Open source cybersecurity is promising, given domestic strengths and international reputation. Priority technology areas for the Netherlands include AI-enabled threat intelligence, cloud, 6G, cryptography, quantum cybersecurity, given national strengths, pressing needs for more autonomy and business opportunity.

Better action

Experience of over ten years of cybersecurity initiatives shows that we also need 'action for better action' to ensure flexibility, relevance, and impact (for potential negative impact see Figure 10 about potential incidents). Therefore:

1. **Continuously improve evidence base:** cybersecurity market surveys and impact assessments; further research on de-risking, economic security, and mutual interdependency.
2. **Adapt to the evolving reality:** institutionalize pro-active monitoring and adaptive response to deal with geopolitical and technological changes.
3. **Deepen synergies:** design packages of actions such that they have mutual leverage, given limited resources and in

order to respond to the similar strategy of geopolitical competitors.

4 **Political and operational accountability:** include delivery of cybersecurity sovereignty in dialogues between top political and operational level, commit to regular democratic reporting.

5 **Improve understanding:** pro-active and planned learning, since cybersecurity sovereignty is vulnerable to unintended consequences, e.g. in resilience vs autonomy, convenience vs security.

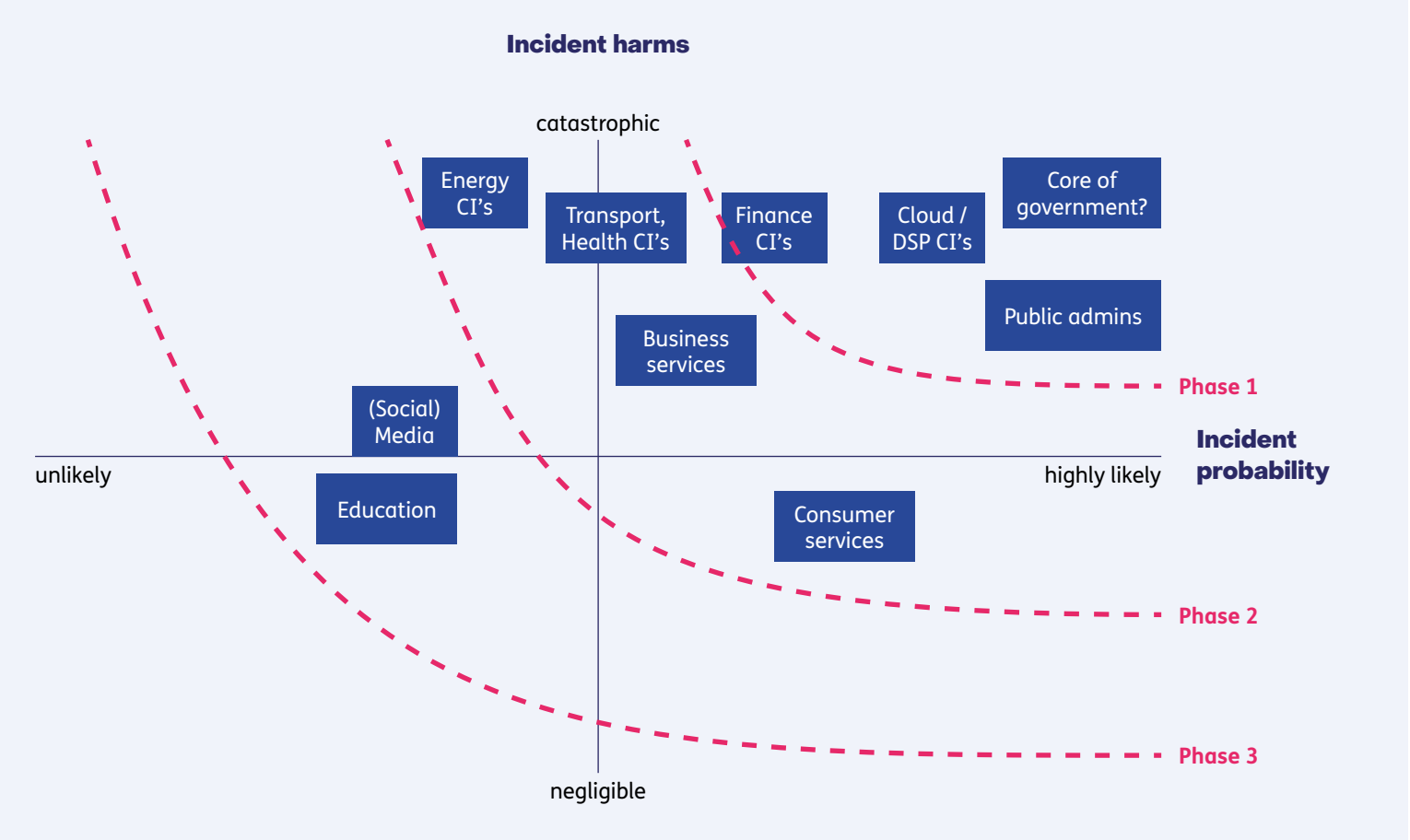

Figure 10 *Potential incidents*

5. Measures to become more digital sovereign

5.1 Summary of the findings

This study indicates that Europe and the Netherlands are dependent on a limited number of non-European stakeholders on most of the digital technology layers for R&D and commercialisation. However, digital layers on which the EU still plays on important role are: (Micro)chips, and on the Networks and Connectivity layer mainly for Telecom (and Mobile Networks). Besides that experts indicate that chances can be created on the Edge Infrastructures and on the Data Sharing Infrastructures by building on the various European initiatives. Other important chances are mainly provided by future technologies such as Quantum technology and 6G.

The European Commission and the Member states have measures in place on almost all technology layers to strengthen the digital sovereignty. Instruments that are most often applied for this are regulation and financing of innovation.

5.2 Available instruments

We distinguish 3 types of instruments that can stimulate digital sovereignty. These are instruments applied by: 1. the government 2. of companies and 3. Research Institutes. In this section they are discussed.

Existing instruments of the government

There are four governmental roles and instruments that are executed or can be executed by policy makers to stimulate digital sovereignty (see Figure 11[317]).

Each of the instruments are discussed below[318];

Regulator

As a regulator, the government initiates a desired behaviour by prescribing or prohibiting certain activities by means of rule- and norm-setting (e.g. based on the carrot and stick). Being a regulator is one of the EU's greatest strengths to set global technical standards in a number of fields (called "the Brussels effect"). Accordingly, the strive for "sovereignty" has a clear connection with the European Commission's "coordinated European approach" including its regulatory efforts towards completing the digital single market. Digital sovereignty based on a comprehensive regulatory program is expected to provide European developers and manufacturers with a competitive edge, and consumers and users with products adhering to high ethical, democratic, and human-rights. As a regulator various instruments can be applied:

- 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 choices on innovation and governance. The EU wants to deliver on the promise of human-centered and risk-based new tech regulation, together with a comprehensive regulatory packaging such as the European Digital Strategy, the European Data Strategy, the Digital Services Act, the Digital Markets Act, AI act etc. The EU has however a harder time in setting global rules and red lines, with regulation being criticized for limiting innovation[319].
- Standardisation[320]: is also an important instrument to fulfil the regulator role. The European Commission developed for instance a Standardisation Strategy outlining their approach to standards within the Single Market as well as globally. This strategy aims to strengthen the EU's global competitiveness, enable a resilient, green and digital economy and to enshrine democratic values in technology applications. Standards help manufacturers ensure the interoperability of products and services, reduce costs, improve safety and foster innovation. Standards give confidence that a product or a service is fit for purpose, is safe and will not harm people or the environment. Compliance with harmonised standards guarantees that products are in line with EU law.

317 Based on and further extended: https://www.kimnet.nl/binaries/kimnet/documenten/notities/2018/09/03/nieuwe-tijden-nieuwe-overheidsinstrumenten/Nieuwe+tijden+nieuwe+overheidsinstrumenten.pdf

318 Stolwijk, Punter et al. (2022), Bridging the Dutch and European Digital Sovereignty gap: https://publications.tno.nl/publication/34639349/urAkBu/TNO-2022-R10507.pdf

319 To shush AI Act critics, the EU fine-tunes innovation pitch – POLITICO

320 New approach to enable global leadership of EU standards promoting values and a resilient, green and digital Single Market: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_661

- Monitoring: if laws are applied correctly is an important complementary instrument (e.g. for the aforementioned regulation for the digital domain).[321] But monitoring of the European Commission can be seen broader and also concerns for instance the measurement of the progress of the digital transformation in the Member states.[322]
- Enforcement[323]: is closely related to monitoring because if (EU) law is not properly applied corrective measures are needed. While the Commission launches infringement procedures in line with its enforcement policy, it also places great emphasis on prevention. An example is that the European Commission fined Google (e.g. for breaching EU antitrust rules).

Facilitator

As a facilitator, the government creates conditions that allow third parties to encourage desired behaviour. The European Commission and the Member states apply facilitation instruments such as:

- The European policy makers provide various financial instruments that contribute direct or indirect to digital sovereignty. Such as[324]: The Digital Europe Programme, Horizon Europe, Connecting Europe Facility (CEF) Public procurement of innovation is another instrument, that can be applied in the digital domain when the public sector uses its purchasing power to act as early adopter of innovative solutions which are not yet available on large scale commercial basis.[325]
- European governments also stimulates skills development. Examples are[326]:
  - The Digital Education Action Plan (2021-2027).
  - Digital Education Hub to cooperate and exchange in digital education at the EU level.
  - The European Digital Skills and Jobs Platform.
  - All Digital supports Europeans that have an insufficient level of digital skills.
  - Train-the-trainer programs via for instance Digital Innovation Hubs and alike.
- European policy makers organise matchmaking between stakeholders. This happens for instance by bringing key stakeholders together interested in future calls for proposals focused on specific digital technologies.[327]
- 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) 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 executes public procurement. This refers to the process by which public authorities, are purchasing work, goods or services from companies. To create a level playing field for all businesses across Europe, EU law provided minimum harmonised public procurement rules. The public sector can apply procurement to boost jobs, growth and investment, and to create an economy that is more innovative, resource and energy efficient, and socially-inclusive. This

321 Enforcement: Frequently Asked Questions: https://ec.europa.eu/commission/presscorner/detail/en/memo_12_12
322 2030 Digital Decade: Commission adopts indicators to monitor Europe's digital transformation and issues guidance to Member States https://digital-strategy.ec.europa.eu/en/news/2030-digital-decade-commission-adopts-indicators-monitor-europes-digital-transformation-and-issues
323 Enforcement: Frequently Asked Questions: https://ec.europa.eu/commission/presscorner/detail/en/memo_12_12
324 Stolwijk, Punter et al. (2022), Bridging the Dutch and European Digital Sovereignty gap: https://publications.tno.nl/publication/34639349/urAkBu/TNO-2022-R10507.pdf
325 Innovation Procurement: https://procure2innovate.eu/innovationprocurement/#:~:text=Public%20Procurement%20of%20Innovative%20solutions%20(PPI)%20happens%20when%20the%20public,on%20large%20scale%20commercial%20basis.
326 Stolwijk, Punter et al. (2022), Bridging the Dutch and European Digital Sovereignty gap: https://publications.tno.nl/publication/34639349/urAkBu/TNO-2022-R10507.pdf
327 An example 5G for Smart Communities – CEF Digital call matchmaking: https://digital-strategy.ec.europa.eu/en/events/5g-smart-communities-cef-digital-call-matchmaking

means that this instrument could also be applied for the digital domain as long as it meets the European procurement rules.

Communicator

As a communicator, the government has an informative role on topics such as digital sovereignty. There are several instruments to execute this role such as

Awareness creation via communication and information campaigns such as the document on Shaping Europe's digital future and based on various speeches that are also published.

Another instrument concerns the vision and strategy development. These strategies and visions are in place to help achieve and communicate about the long-term digital transformation needed. There are several strategies and visions published by the European Commission such as the European Digital Strategy[328], the EU strategy on Web 4.0 and virtual worlds to steer the next technological transition[329] , the European Strategy for Data.[330]

New instruments of the government

Next to the existing instruments, the government also has some new instruments to stimulate digital sovereignty, such as:

- R&D and innovation instruments resulting in technology breakthroughs (e.g. in AI, quantum, new materials).
- The national growth fund initiatives in the Netherlands to stimulate the economy and to become more sovereign in certain technological areas, such as in the NextGen High-tech growth fund.
- Important Projects of Common European Interest (IPCEIs)[331], which are integrated European projects consisting of several national projects executed by companies and/or research institutes from different EU Member States that are complementary, and contribute to strategic European goals such as digitalisation, sustainability and sovereignty. Through IPCEIs, much larger sums than for other state aid exemptions can be awarded.
- Synergistic initiatives in which sectors cooperate such as a combined action between the manufacturing and defence sector. An example of an activity based on cross-sectoral cooperation is the Dutch NXTGEN High-tech growth fund.[332]

Instruments of companies

Also companies have various instruments to stimulate their digital sovereignty such as:

- The corporate strategy is a unique long-term plan or framework that outlines the direction that a company will take in order to achieve its goals. It defines a mission and vision for the whole organization, to create value, develop competitive advantage, and seize maximum market share. A corporate strategy helps companies to identify trends and opportunities, encourages innovation, offers a competitive advantage in the market, and optimizes the business model. A roadmap with clear activities to ensure digital sovereignty of the firm might be part of this strategy (e.g. including how to store and use the data based on which technologies and providers). Various companies are already doing that .[333]
- A digital / IT strategy of a company is the plan for introducing and using digital technology to meet a firms business goals. Also this strategy can contain the policy measures of a firm to ensure digital sovereignty, while taking the business value into account. Various companies indicated that their digital sovereignty strategy is driven by the business value.[334]
- Measures to deal with the increasing complexity (such as exchanging best practises with partners and hiring consultants for advice) are getting more and more important for companies in stimulating their digital sovereignty. The complexity is two-fold. First of all the new digital solutions are becoming more advanced and introduce new complexities and require decisions of CIOs about their digital infrastructure and about the way they share their data. These decisions have an impact on their digital sovereignty.

328 EU: An overview of the European digital strategy: https://www.dataguidance.com/opinion/eu-overview-european-digital-strategy
329 Towards the next technological transition: Commission presents EU strategy to lead on Web 4.0 and virtual worlds: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3718
330 A European Strategy for data: https://digital-strategy.ec.europa.eu/en/policies/strategy-data
331 https://www.rvo.nl/subsidies-financiering/ipcei
332 Growth fund NXTGEN HIGHTECH: https://hollandhightech.nl/en/current-dossiers/our-dossiers/nxtgen-hightech
333 Based on expert interviews
334 Based on interviews

Next to that the regulation is increasing, which increases the complexity as well and requires legal expertise. Large organisations have legal experts in house who can support the CIOs. However, this is a challenge for SMEs who often do not have this expertise.
- Besides that CIOs are recommended to not only follow European initiatives (e.g. around cloud and data spaces), but also to actively participate in those initiatives. This enables them to influence the direction of these initiatives and directly benefit from their results.

Instruments for Research Institutes

Next to that also the Research Institutes have a diverse set of instruments to stimulate the digital sovereignty of Europe, the Netherlands, companies and citizens, such as:

- Technology development: The Research Institutes are active on the development of technological solutions that stimulate digital sovereignty. Examples of such technological solutions are quantum technology, 6G, decentralized data infrastructures, Data Spaces etc.
- Ecosystem development / orchestrating: The Research Institutes are also active as independent intermediary in orchestrating ecosystems active on joint innovation projects to stimulate digital sovereignty.
- Standards setting: Research Institutes are furthermore setting and stimulating the relevant standards, which are based on digital sovereignty principles. These standards concern technical standards, but also relate to legal and ethical norms.
- Neutral advice: Research Institutes also function as parties that can provide neutral advice on how to become more digital sovereign based on technological, policy and business solutions.

5.3 What if we want to become fully digitally sovereign?

Let's first qualify what fully digitally sovereign means. This is not about autarky, that is, it is not about doing all on our own as EU (taking 'we' and 'us' and 'our' as referring to the EU). Rather, this is about ensuring that we have our voice in our own future by having – in the digital domain - sufficient knowledge, development, production and usage capability and capacity and under our own control in the EU. This does not at all imply that as EU we cannot sufficiently realise our digital sovereignty if we have dependencies on others. However, these third countries should be respectful partners, that is they should not pose a threat to our sovereignty. These partners must be sufficiently likeminded and must respect our justified wish for sufficient knowledge, jobs, companies, wealth and respect for our values in the future, in the near-term and in the long run. We do not need autarky. We must keep protectionist tendencies in check and, as Dani Rodrik argues, "where we have economic nationalism we need to do it the right way".[335]

With the explanation above and the aforementioned instruments in mind this section will focus on what is needed to become **in this sense** fully digitally sovereign. We are well aware, however, that for Europe and the Netherlands to become fully sovereign ambitious measures are required and generally these should be joined up. The following longlist of possible 'ambitious measures' is proposed by the involved experts for each of the following technologies[336].

Cyber security:

- Realize full cybersecurity sovereignty with European and politically-accepted international partnerships. This means having full capabilities, capacities and control over the design and use of the technology relevant for cyber security.
- Make the regulatory landscape for cybersecurity easier to navigate for companies.
- Sovereignty by default in public procurement, with comply and explain.
- Set-up a PPP for scale-up risk capital in cybersecurity.

AI/Intelligence:

- Ensure systematic and extensive R&D in and roll-out of AI, including privacy-by-design. This can be done for instance through IPCEI-alike instruments.
- Create an European AI register for accountability; to hold organizations accountable for the algorithms and software they use and ensure that they are transparent and fair.
- Mandate companies to report on their measures to ensure privacy by design.
- Create leverage from the AI program to ensure uptake by European companies (especially SMEs).
- Invest heavily and completely integrate the investments within the EU and avoid separate initiatives per country, they are just too small.

335 https://www.project-syndicate.org/commentary/east-asian-model-vindicates-economic-nationalism-by-dani-rodrik-2023-11.
336 These measures are based on expert input.

- In public procurement require European AI, unless explained why this is not the right choice.

Data:
- Provide financial incentives for data sharing in sectors of public interest such as health and the energy and environment domain.
- Provide regulation for mandatory free data portability.

Data Sharing Infrastructures:
- Extend eIDAS 2.0 to trust service providers in other areas such as for the identification of equipment.
- Ensure mandatory eIDAS implementation across enterprise and public services.
- Provide EU wide public procurement requirements for using the outcomes of Simpl and other relevant EU investments.
- Ensure mandatory participation in data spaces based on regulation.
- Provide R&D funding for managing future complexity of data spaces in combination with regulation for the internal market.
- Comply and explain to services added to Gaia-X.

Cloud Infrastructures:
- Introduce a 'comply or explain' regime for the mandatory use of EU-regulated cloud infrastructures in the public sector and other services of public interest.
- Provide scale-up funding for EU-based cloud infrastructures.
- Extending internet tax-regimes to avoid that data can be collected by data centers about anything with or without a purpose.

Edge Infrastructures:
- Develop a cloud-edge infrastructure strategy.
- Address edge interoperability as a market requirement – via R&D to stimulate interoperability and compliance with market access and competition requirements for the internal market
- Provide R&D funding to manage the future complexity of the cloud-edge continuum.
- Provide mandatory public procurement specifications.
- Develop regulation on embedded edge devices: compulsory standards, compulsory regulation

Telecom (mobile networks):
Initiate an IPCEI and public policy initiative on European telecom equipment, including not only R&D but also go-to-market actions such as mandatory public procurement specifications and make a link with regulation.

Make sure there is a mandatory multi-cloud requirement (with at least 1 European cloud) for cloud-based 5G and 6G networks.

Internet Cables and Satellites:
- Ensure large investments in a secure connectivity agenda proposed by the EC, combining a diversification of internet connections and satellite-based communications.
- Prohibiting the use of non-regulated satellite infrastructures for critical purposes such as navigation, media, emergency services.

(Micro)chips:
- Provide talent initiatives dedicated to (micro)chips
- Provide talent and companies for chip design, not only in the 'nodes' that we now have in the EU, but also the advanced nodes.
- Ensure the manufacturing of all type of chips in the EU, the EU currently cannot create smaller chips than 32 nm.
- Ensure packaging by the EU, which is currently only possible for small series. The only company that will have a division in Europe in the future is Amkor (this location will be based in Portugal).
- Tools and consumables needs to be provided by European players.
- Ensure secure and energy efficient quantum and AI chips.
- Develop at EU and NL level a full quantum industrial strategy.
- Increase the accountability of OEMs for microchips included in their products.
- Mitigate the dependence on Chinese players for underlying materials.

Again, this overview is a list of potential, often ambitious, measures needed to become fully digital sovereign.

5.4 What is the current policy landscape?

We are not in a greenfield situation when it comes to policies for digital sovereignty. There are currently various policy measures in place. For almost each of the technology layers on European level and also on national level policy measures can be distinguished as described in the policy sections of Chapter 2, examples of these measures per technology layer are:

Intelligence:

- AI Act[337]: The AI Act provides direction for developers to comply with the requirements. Within so-called regulatory sandboxes, the developers can use this to innovate. In this way, AI applications can be developed in the EU and can improve our technological position on the global market and ensure high-quality AI. AI in, for example, design programs, applications in the manufacturing industry and in video games can be stimulated in this way.

Data:

- EU Strategy for data[338]: The European strategy for data aims at creating a single market for data that will ensure Europe's global competitiveness and data sovereignty since data is an essential resource for economic growth, competitiveness, innovation, job creation and societal progress in general.
- Open Data directive[339]: The Open Data Directive mandates the release of public sector data in free and open formats. The overall objective of the Directive is to continue the strengthening of the EU's data economy by increasing the amount of public sector data available for re-use, ensuring fair competition and easy access public sector information, and enhancing cross-border innovation enabled by data.
- GDPR[340]: The General Data Protection Regulation (GDPR) is the toughest privacy and security law worldwide. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people within the EU.

Data Sharing Infrastructures:

- EU Strategy for data: see under data.
- Data Governance Act[341]: The Data Governance Act aims to increase trust in data sharing, strengthen mechanisms to increase data availability and overcome technical obstacles to the reuse of data. It also supports the set-up and development of common European data spaces in strategic domains, involving both private and public players, in sectors such as health, environment, energy, agriculture, mobility, finance, manufacturing, public administration and skills.
- European digital identity framework[342]: By providing a harmonized system all over the EU, the new rules move far beyond the existing cross-border legal framework for trusted digital identities, the European electronic identification and trust services initiative (eIDAS Regulation). The currently applicable eIDAS provides the basis for cross-border electronic identification, authentication and website certification within the EU.
- Data Spaces[343]: The EU stimulates the set-up of Common European data spaces. These data spaces will ensure that more data becomes available for use in the economy and society, while keeping companies and individuals who generate the data in control.
  - Simpl[344]: Simpl is the smart middleware that will enable cloud-to-edge federations and support major data initiatives funded by the European Commission, such as common European data spaces.

Cloud & Edge infrastructures:

- Digital Markets Act (DMA)[345]: Some large online platforms act as "gatekeepers" in digital markets. The Digital Markets Act aims to ensure that these platforms behave in a fair way. These rules establish obligations for gatekeepers, "do's" and "don'ts" they

337 Voorlopig politiek akkoord EU-eisen ontwikkeling kunstmatige intelligentie: https://www.rijksoverheid.nl/actueel/nieuws/2023/12/09/voorlopig-politiek-akkoord-eu-eisen-ontwikkeling-kunstmatige-intelligentie
338 EU Strategy for Data: https://dataeconomy.eu/eu-data-strategy-2020/#page-content
339 Open Data Directive: https://data.gov.ie/pages/open-data-directive
340 GDPR: https://gdpr.eu/what-is-gdpr/
341 European Data Governance Act: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act
342 European Digital Identity: https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_2664
343 Common European data space: https://dataspaces.info/common-european-data-spaces/#page-content
344 Simpl: https://digital-strategy.ec.europa.eu/en/node/10891/printable/pdf
345 Digital Markets Act: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

must comply with in their daily operations.
- Digital Services Act (DSA)[346]: The rules specified in the DSA primarily concern online intermediaries and platforms. For example, online marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms.
- Important Project of Common European Interest on Next Generation Cloud Infrastructure and Services (IPCEI-CIS)[347]: 12 EU Member States have joined forces in the European IPCEI-CIS project to create a common cloud & edge infrastructure for Europe.

Networks & Connectivity:
- 5G and 6G R&D investment policy: There are various investment programs of the EU and the Member States. For more details see section 2.2.
- EU Secure Connectivity Programme[348]: The secure connectivity programme will provide enhanced satellite communication capacities to governmental users, businesses as well as citizens. It aims to deploy an EU satellite constellation – IRIS² (infrastructure for resilience, interconnectivity and security by satellite) – to support a wide variety of governmental applications, mainly in the domains of situational awareness (e.g. border surveillance), crisis management (e.g. humanitarian aid) and the connection and protection of key infrastructures (e.g. secure communications for EU embassies).

(Micro)chips:
- EU Chips Act[349]: The European Chip Act will strengthen the semiconductor ecosystem in the EU, ensure the resilience of supply chains and reduce external dependencies. It is an important step for the EU's technological sovereignty.
- Building manufacturing facilities for chips[350]: Fabrication facilities of Intel and TSMC will be built in Germany.

5.5 Current policy is not enough to address future needs

To realize the ambition presented in section 3.7- to get more technologies in the Open International Collaboration scenario – we feel that additional measures will be required. Without additional measures it will be challenging to counteract the movement towards Big tech dominance scenario. Based on the expert consultation the following (additional) measures are recommended:

- **Prioritize focus areas since some technologies require more attention than others (e.g.);**
- For Data Sharing Infrastructures and Cloud and Edge Infrastructures the ambition is to move them (a bit) from the Big Tech dominance scenario towards the Open International Cooperation (see Figure 9). For dedicated measures relevant for these technologies see Box 1.
- Telecom (Mobile Networks) remains in the Competing Coalitions scenario, but will move to the upper left corner of this scenario and Intelligence is expected to split between the Unilateral Approach and the Open International Coopertion.
- For the other technologies the ambition is to keep their current position, which is in various cases a challenge in itself (see Figure 9).

346 Digital Services Act: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
347 IPCEI CIS: https://opennebula.io/innovation/ipcei-cis/
348 EU Secure Connectivity Programme: https://commission.europa.eu/strategy-and-policy/eu-budget/performance-and-reporting/programme-performance-statements/eu-secure-connectivity-programme-performance_en
349 EU Chip Act: https://digital-strategy.ec.europa.eu/nl/policies/european-chips-act
350 German budget woes threaten chip fab funding for Intel and TSMC: https://www.theregister.com/2023/11/24/german_budget_woes_threaten_chip/

Box 1 Measures to reach the ambition (see Figure 9), of which some of them are also needed as part of the ambitious measures (see section 5.3):

Measures for Data Sharing Infrastructures:

- Ensure mandatory eIDAS implementation across enterprise and public services.
- Provide EU wide public procurement requirements that may include the use of Simpl.
- Ensure mandatory participation in data spaces based on regulation.
- Provide R&D funding for managing future complexity of data spaces in combination with regulation for the internal market.
- Stimulate the focus on the value proposition and business model of the data spaces by making this compulsory in EU calls (e.g. that are focused on the set-up of data spaces).

Measures Cloud and Edge Infrastructures:

- Provide scale-up funding for EU-based cloud infrastructures.
- Develop and edge infrastructures strategy.
- Provide R&D funding to manage the future complexity of the cloud-edge continuum.

It is important to keep in mind that:

- If a Big Tech company such as Microsoft was a country, it would be one of the richest nations in the world with a value larger than the GDPs of countries like Canada, Russia and Spain.[351]
- The EU investments in the digital domain are much lower than for instance in the US. The US is for instance at the forefront of private funding for AI, with over $29 billion invested in the sector last year.[352] China closely follows, with investments reaching almost $10 billion. However, the EU lags behind with investments totaling just over $2 billion.[353]

That means that Europe needs to realize that the ambition for digital sovereignty as presented in Figure 9 comes with a price to catch up and create own European strengths. However, to quantify this future research should focus on the quantification of the costs and benefits of digital sovereignty.

351 Companies that are worth more than countries: https://www.realbusinessrescue.co.uk/advice-hub/companies-worth-more-than-countries

352 Europe Lags Behind US and China in AI Investment: https://www.toolify.ai/ai-news/europe-lags-behind-us-and-china-in-ai-investment-1240980

353 Ibid

- **Move the main focus from protecting the digital domain based on backward regulation, towards looking forward;**
- Currently many regulations are driven by negative effects experienced by digitalization. Another additional could be to focus on forward looking policy and early preparation of regulation, providing a framework for (the acceleration of) new innovations.
  - By focusing on investment in ecosystem development and business cases of future technologies such as data spaces, quantum driven solutions, 6G etc. This can be done by making ecosystem development and business model development more explicitly part of future EU calls.
  - Relaxing antitrust law and state aid rules (e.g. enforced by regulatory sandboxes and via IPCEIs) to stimulate joint innovation and development of like-minded partners on the aforementioned digital technology layers.
  - Apply tax-free R&D for digital technology developments that are of high strategic importance (such as future technologies like quantum).
  - By stimulating more venture capital for European champions.

- **Create control points on each of the digital technology layers;**
  - In the form of unique business activities that are difficult (or impossible) for players in the value chain to avoid.
  - Or by ensuring crucial links in value chains that are difficult to replace and that are in combination very knowledge intensive. Such links could be fulfilled by companies, products, standards and applications.
  - This requires a clear analysis and overview of potential control points in combination with a clear agenda on what needs to be done per digital technology layer by whom to come to these control points.

- **Ensure that digital technologies are affordable, efficient, resilient, safe and in line with the Sustainable Development Goals (SDGs):**
  - **Affordable and efficient;** means that organizations are not dependent on individual digital players or countries, but can negotiate fair prices and conditions, and use state-of-the-art technologies that ensure efficiency.[354]
  - **Resilience; concerns** the ability to prevent, respond and quickly recover from events that have the potential to disrupt such as delivery issues in supply chains. Digital technologies enable this resilience.
  - **Safety:** concern safe and cyber secure digital solutions.
  - **In line with the Sustainable Development Goals (SDG),** respect privacy, sustainability and health.

- **Apply the 3 Ps (Promote, Protect, Partner) to come to a digital sovereign and competitive European market;**
  - **Promote the strengths of Europe and the Netherlands in the digital domain and build on them.** An example of such a strength is equipment manufacturing, in particular complex equipment which require high precision production. The market for such products will expand when moving in to the digital anything – everywhere domain. Examples are mobility, healthcare, manufacturing equipment and the built environment. As the equipment becomes much more digital, the Netherlands and Europe have the potential to take the lead in this area.
  - **Protect European values** by avoiding that hate speeches go viral, avoiding that Big-Tech controls other countries, respecting democratic values and privacy based on the harmonization of current regulation and potential future legislation.
  - **Partner with counties that are trusted partners and share the same values** to strengthen and support each other in becoming more digital sovereign.

- **Apply a system of continuous monitoring and corrective actions based on which;**
  - Required changes in policy instruments can be implemented.
  - Prioritization of focus technologies might change over time.

- **Come to a holistic policy approach to ensure that the policy instruments complement and strengthen each other;**
  - This requires cooperation among various governmental institutions within the European Commission, among Member States, within Member States, as well as on global level among like-minded partners who share the same norms and values.
  - The aforementioned continuous monitoring and corrective actions can support in this.

354 Digital Sovereignty: Why it pays to focus on independence in digital transformation - PwC

- **Make policy instruments (e.g. the carrot and stick) more proportional to the goal that needs to be achieved with it e.g.;**
  - If Big Tech receives a fine for harming specific European values, make sure that the fine is proportional to the harm to avoid that the fines become a 'cost of doing business that is incorporated in the price for the end user'.

5.6 Concluding remark

Based on this report we can conclude that Europe and the Netherlands are becoming ever less digital sovereign, even if counter-acting policy measures have been taken on almost all digital technology layers. The reason is that becoming digital sovereign is a multidisciplinary issue for which there is no quick fix, most measures are only relative recently taken, and there is still a lack of focus on digital sovereignty in digital policy. Digital sovereignty comes with a price and requires:

1. **A long term investment in multiple measures** by policymakers, the industry and Research Institutes.
2. **A continuous monitoring and corrective action system to come to measures that are proportional and adaptive** to the underlying problem.
3. **A balancing act to become Digital Open Strategic Autonomous:** by moving more digital technologies towards the Open International Cooperation scenario, while avoiding protectionism and fostering democracy.

Contact details

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

Claire Stolwijk
claire.stolwijk@tno.nl

Julian Rabbie
julian.rabbie@tno.nl

Matthijs Punter
matthijs.punter@tno.nl

David Regeczi
david.regeczi@tno.nl

Paul Timmers
paul.timmers@iivii.eu

Simon Dalmolen
simon.dalmolen@tno.nl

TNO Vector
Centre for Societal Innovation and Strategy

Acknowledgement
We want to thank the following experts for their feedback: Rogier Verberk, Freek Bomhof, Pieter Nooren, Toon Norp, Hans Stokking, Erik Langius, Edwin Harmsma, Elmer Rietveld, Thijmen van Bree, Sylvie Dijkstra-Soudarissanane.

tnovector.nl