Baischew, Dajan; Kroon, Peter; Lucidi, Stefano; Märkel, Christian; Sörries, Bernd

Research Report

Digital sovereignty in Europe: A first benchmark

WIK-Consult Report

Provided in Cooperation with:
WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH, Bad Honnef

Suggested Citation: Baischew, Dajan; Kroon, Peter; Lucidi, Stefano; Märkel, Christian; Sörries, Bernd (2020) : Digital sovereignty in Europe: A first benchmark, WIK-Consult Report, WIK-Consult GmbH, Bad Honnef

This Version is available at:
https://hdl.handle.net/10419/251539

WIK-Consult • Report

Study for Squire Patton Boggs (US) LLP

Digital Sovereignty in Europe – a first benchmark

Authors:
Dajan Baischew
Peter Kroon
Stefano Lucidi
Christian Märkel
Bernd Sörries

WIK-Consult GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Germany

Bad Honnef, 3rd December 2020

Imprint

WIK-Consult GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Germany
Phone: +49 2224 9225-0
Fax: +49 2224 9225-63
eMail: info@wik-consult.com
www.wik-consult.com

Person authorised to sign on behalf of the organisation

General Manager	Dr Cara Schwarz-Schilling
Director Head of Department Postal Services and Logistics	Alex Kalevi Dieke
Director Head of Department Networks and Costs	Dr Thomas Plückebaum
Director Head of Department Regulation and Competition	Dr Bernd Sörries
Head of Administration	Karl-Hubert Strüver
Chairperson of the Supervisory Board	Dr Daniela Brönstrup
Registered at	Amtsgericht Siegburg, HRB 7043
Tax No.	222/5751/0926
VAT-ID	DE 123 383 795

Contents

Executive summary

A "geopolitical Commission" seeking strategic autonomy.

The EU and its Member States are facing an increasingly complex context of international relations. The von der Leyen Commission recognized this from the outset. Already in her first press conference she made clear that she will lead a "geopolitical Commission". The recent stances towards "strategic autonomy" and "digital sovereignty" have to be interpreted against this background.

The COVID-19 crisis has not only accelerated the progress of digitalisation and shown how crucial our ICT infrastructure is, but it has also increased awareness of the consequences of being dependent on foreign suppliers of critical services and products. Thus, the pandemic also accelerated the trend towards gaining strategic autonomy with policymakers in the major economic blocs globally (US, Asia and Europe). Given the prominence of digitalisation during the pandemic, it is not surprising that within the public debate around strategic autonomy, "digital sovereignty" is often in the spotlight. As part of the wider debate, digital sovereignty tends to refer to concerns about the autonomy of crucial national ICT infrastructure and the control individuals have over their own data.

These concerns emerge from an ever growing importance of digitalised critical infrastructure, an increasing centrality of mobile telecommunications networks for the functioning of businesses and society as well as an apparent lack of control over data on both the individual and the collective (national and supranational) levels. Notwithstanding the fundamental contradiction of digitalisation and sovereignty in the traditional sense of the concept, policymakers across Europe seek to (re-)gain control over a transition that is dominated by firms originating outside of Europe.

Digital sovereignty – not a uniform concept.

Based on published positions, statements and reports on the EU-level as well as for each of the 27 Member States and the UK, we find that digital sovereignty is not a uniform concept. Policymakers attribute various rationales and objectives to it and they use similar or different terms in its place, e.g., technology sovereignty which can mean similar or different things. This lack of concurrence could ultimately be an impediment to turning the ambition of digital sovereignty into reality.

Our analysis, however, suggests that despite marked differences three common dimensions of digital sovereignty exist: (1) privacy, (2) cybersecurity and (3) strategic. Whilst the first dimension revolves predominantly around the individual ability to control their digital lives and data, the second and third dimensions refer mostly to the collective level of states' as well as the EU seeking to (re-)gain control and leadership in the digital age.

The strategic dimension of digital sovereignty only recently gained prominence.

The three identified dimensions can be traced along the public debate around digitalisation, in which we find that the dimension of cybersecurity was the earliest to emerge as a primary concern of policymakers. With increasing adoption and dominance of largely US-American consumer-oriented online services offered at no monetary cost, but using the personal data of millions of European citizens, the second dimension "privacy" came into focus. In recent years, amid the geopolitical situation and the pandemic, the strategic dimension appears to gain the most traction in the public debate.

Besides developing the own capacities and critically reviewing services and product from non-European suppliers in crucial ICT infrastructure, also the financial instrument of restricting foreign direct investments (FDI) is discussed to curb non-European influence. Next to central measures on the EU-level, Finland, Italy and Germany are examples of countries that have already taken FDI measures. However, due to its capital intensity and growth opportunities, capital investors (European and non-European) have always played an important role in the European ICT sector and will most likely continue to do so in the future.

France and Germany drive digital sovereignty in Europe.

In the benchmark, we find differences in how the three dimensions of digital sovereignty reflect in the positions and policy initiatives of individual Member States as well as the UK. Around half of the EU Member States still follow a narrow interpretation of digital sovereignty predominantly along the lines of cybersecurity. In Western Europe and in the Nordics the dimension of cybersecurity is supplemented by the privacy dimension. For the European economic heavyweights France and Germany as well as digital leaders such as Denmark and Estonia the concept of digital sovereignty encompasses all three dimensions whilst the strategic dimension appears to dominate at the moment. The same is true on the EU-level. However, France and Germany stand out and apply the broadest scope of digital sovereignty as their strategy papers lift the concept even to being a matter of defending European values such as freedom, solidarity and tolerance.

A strategic stance towards digital sovereignty fosters a proactive approach.

Based on our review of official statements and policy documents, we find that the approach towards digital sovereignty varies across countries. While some countries propagate a proactive approach, others follow a reactive one. "Proactive approach" in this context means that extensive economic policy or geopolitical measures are taken to reduce dependency on foreign or rather non-European providers (examples include the creation of European cloud services, exclusion of certain providers of infrastructure and services and the establishment of data embassies , etc.). In contrast, a "reactive" approach is characterised by adopting a reactive stance against cyberattacks and/or

following EU policy. These countries primarily try to take protective measures and refrain from economic policy measures with a high degree of intervention. In line with their emphasis on the strategic dimension of digital sovereignty, France and Germany follow a proactive approach. So do Denmark and Estonia.

Limiting non-European suppliers for 5G; fostering existing alliances.

The restrictions put in place to limit or exclude certain vendors from the rollout of 5G networks in some Member States and most prominently in the UK represent probably the most obvious example of countries seeking to limit non-European influence in the context of digital sovereignty.

On 22 March 2019, the European Council called for a coordinated approach to the cybersecurity of 5G networks. Thereafter, in particular, Huawei and ZTE – the Chinese competitors of the European suppliers Ericsson and Nokia – have come under the scrutiny of policymakers and regulators throughout the EU as well as in the UK.

We observe that the actual measures taken vary across the countries analysed in the report. They appear to be guided by existing economic and geopolitical alliances. For instance, the UK and Ireland have taken rather strong measures against Chinese vendors of network equipment. Both countries have long-established links to the US and, in the case of Ireland, depend on the influx of taxes from various US tech companies' EU headquarters. Similarly, countries that for historical and/or strategic reasons want to protect themselves from stronger Russian influence (such as PL and EE) tend to maintain closer cooperation with the US on ICT security issues. Germany, on the other hand, appears to have a more neutral approach to vendor selection for its 5G deployment. Underlying reason could be that the country has to strike a balance between its good relations with the US and the importance of the Chinese market for some of its major industries.

The Digital Single Market: Already striving for EU digital autonomy and leadership.

The concept of digital sovereignty transpires already from many of the initiatives under the Digital Single Market as they essentially aimed to increase the digital autonomy of the EU and (re-)claim leadership in key fields of the digital transformation.

Regarding the cybersecurity dimension, the European Union Agency for Network and Information Security (ENISA) published in 2015 and 2016 guidance on the identification of Critical Information Infrastructure (CII) assets and services which targeted Member States that were at the beginning of CII protection structure development or were looking to further improve existing structures. In August 2016, the Directive on security of network and information systems entered into force. Besides providing the legal base, the EU will also create a network of European centres of cybersecurity expertise,

in order to reinforce these capacities in the EU. Cyber security, which combines digital capabilities with national sovereignty, can also be interpreted as an effort towards digital sovereignty.

Regarding the strategic dimension, the European Commission launched strategies and investments regarding artificial intelligence and robotics to boost the EU's research and industrial capacity as these technologies are considered key drivers of future innovation and economic growth. Furthermore, the Euro High Performance Computing Joint Undertaking was established in 2018 aiming to equip Europe with a world-class supercomputing infrastructure, which will support leading R&D in many sectors.

The current Commission doubles down on gaining digital leadership.

The current Commission carries forward these initiatives and increases the drive towards home-grown solutions and digital champions. It seeks to unite the measures of Member States in the key areas of artificial intelligence and data economy with central policy measures and funding. In fact, a substantial share of the €750 billion recovery fund, announced during the Covid-19 crisis, is earmarked for fostering digital economy in the EU.

The plan to create a "single European data space" was one of the first policy initiatives pushing towards the provision of digital tools originating in the EU. Thierry Breton summarised its goal as follows "..*European data will be used for European companies in priority, for us to create value in Europe*."

Most prominently and underscoring their proactive stance towards digital sovereignty, France and Germany are collecting steam around a the European data infrastructure GAIA-X also dubbed "AI-Airbus". The declared aim is to establish a common data infrastructure based on European values. The underlying concern relates to (1) the potential dependency on non-EU and in particular US providers of cloud storage and (2) the potential infringement of data protection when data is stored with US-based providers of cloud storage due to the US Cloud Act. National and European cloud services as well as the data embassy concept (which can be seen as an extension of cloud services) can be considered as European alternatives.

Digital sovereignty is not autarky.

The EU as well as most of the countries analysed appear to be keen in underscoring that neither digital sovereignty nor strategic autonomy push for autarky or protectionism. Clearly, digital sovereignty is about striking the balance between achieving its own autonomy while still maintaining a diversified vendor portfolio and international trade relations, which are so important for many economies in the EU.

1 Introduction

It has become apparent that the COVID-19 pandemic has forced digitalisation into fast forward mode. In some instances, such as the introduction of governmental contact-tracing applications, the spotlight has been put on existing dependencies regarding software and hardware commonly used by citizens and governments alike.

Furthermore, the pandemic has accelerated an already emerging trend towards gaining "strategic autonomy" among policymakers in the major global economic blocs (US, Asia and Europe). The European Parliamentary Research Service defined strategic autonomy as follows: "*The ability to act autonomously as well as to choose when, in which area, and if, to act with like-minded partners. The capacity to act autonomously implies both the ability to decide and to implement decisions in an autonomous manner*".[1] The US, China and the EU aim to increase their economic resilience by becoming less reliant on countries outside their respective areas of immediate influence. While the US appears to follow an openly protectionist stance in achieving resilience under the slogan "America first", and China recently announced becoming more self-reliant as a reaction to the US sanctions with its 'Made in China 2025' strategy, the EU seeks to strike a balance between its objectives of strategic autonomy and sustaining an open and free trade regime fuelling the economies of its largest Member States.

Within the public debate around strategic autonomy, "digital sovereignty" is often in the spotlight when it concerns the autonomy of crucial national ICT infrastructure and controlling one's own data. A trigger for the current prominence of digital sovereignty seems to be the recognition of many EU leaders that the EU is indeed falling behind across many critical fields of technological innovation which will likely be the drivers for future economic growth. For instance, 421 of the Top500 supercomputers globally are not in the EU.[2] The field of artificial intelligence (AI) research is equally dominated by research institutions and companies in the US and China as documented by the number of research publications originating these countries.[3] A similar picture emerges for digital applications and services. US companies have been the leading suppliers of operating systems, online platforms and streaming services to name just a few major

1 Policymakers and officials across Member States as well as from within the EU institutions attach different meanings, hopes, objectives and rationales to the term "strategic autonomy". This has been analysed by several authors. For a recent example see Libek, E. (2019): European Strategic Autonomy: A Cacophony of Political Visions. International Centre for Defence and Security (ICDS).Consequently, we do not feel the need to add to this discussion in the present report. 'Strategic autonomy' is not about self-sufficiency but about means and tools to reduce external dependencies in areas deemed strategic and where dependencies could compromise autonomy, whilst continuing to cooperate with partners in a multilateral setting." (p. 3)

2 See The List of Top500 (55th edition – June 2020). Available at: https://www.top500.org/lists/top500/2020/06/. Notably, 10 of the ranked computers are in the UK and another 3 and 2 are located in Norway and Switzerland respectively.

3 See European Commission (2018): USA-China-EU plans for AI: where do we stand? Digital Transformation Monitor. Brussels. Available at: https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_AI%20USA-China-EU%20plans%20for%20AI%20v5.pdf.

digital domains. The EU has to (re-)gain its digital leadership position. Obviously, industrial data and the imminent fourth industrial revolution can be drivers of such an effort.

On a more fundamental level, it should however be noted that given the fluidity of digital transformation, non-rivalry of digital data use as well as borderless internet, digitalisation seems inherently opposed to the concept of sovereignty which relates to concepts of control, autonomy and defined borders. Similar to strategic autonomy, it seems that with digital sovereignty it is also about finding the right balance.

The present report seeks to contribute to finding that balance by unpacking the objectives and rationales underpinning "digital sovereignty". This is done by analysing the positions, statements and policies of EU Member States and the UK as well as those issued centrally at EU-level. The report refrains from any judgement or evaluation of the policy approaches by any country or the EU bloc. Its objective is merely to provide a descriptive and informative overview of the status-quo as well as a contextualisation, where necessary. By collating the findings in the individual countries as well as the EU bloc, we aim to present high-level patterns as well as insights on potential differences in the apparent underlying conceptualisations of and policy approaches towards digital sovereignty.

The report proceeds as follows:

- **Chapter 2** provides an overview of contemporary quotes by policymakers and high-ranking EU officials reflecting their understanding of the term "digital sovereignty". Using this overview, we present a categorisation of the underpinning rationales and objectives of digital sovereignty which is used for the subsequent analysis of the documents published by EU Member States and the UK as well as those issued centrally at EU-level. Overall, we find that positions towards digital sovereignty vary quite substantially. Nonetheless, three common dimensions can be derived: (1) cybersecurity, (2) privacy and (3) strategic (geopolitical);
- **Chapter 3** elaborates on the European context of digital sovereignty. It describes how digital sovereignty is reflected in the strategy announced by the von der Leyen Commission and how the COVID-19 pandemic emphasised some critical dependencies from non-EU countries. Furthermore, we discuss how the Digital Single Market (DSM) strategy pertains to digital sovereignty;
- **Chapter 4** describes the main findings, categorises common topics across the EU and the UK, and highlights differences between countries regarding the objectives and rationales attributed to digital sovereignty;
- **Chapter 5** presents our concluding remarks; and
- **Chapter 6** the used methodology and the specific country information on digital sovereignty can be found in the **Annexes**.

2 Observed Dimensions of Digital Sovereignty

The term digital sovereignty is not self-explanatory and, in fact, policymakers attribute various rationales and objectives to it. This chapter sets out to shed light on the underpinning rationales and objectives as reflected in official statements. We also draw on these statements to develop a structure, which we apply throughout the report to analyse the different dimensions of digital sovereignty (cybersecurity, privacy and strategic).

2.1 Contemporary quotes on Digital Sovereignty

There are multiple definitions of digital sovereignty and the understanding of its scope differs between countries. Likewise there are various interpretations among policymakers; some use digital and technological sovereignty interchangeably and some argue that they are not the same. Below, an overview of quotations from national and European policymakers concerning the rationales and objectives they attribute to digital sovereignty are sorted by date.

Ursula von der Leyen, President of the European Commission, Inaugural Speech at European Parliament (2020):[4]

"We must have mastery and ownership of key technologies in Europe."

Margrethe Vestager, Executive Vice President of the European Commission for A Europe Fit for the Digital Age and European Commissioner for Competition, Speech at CERRE event on "Digital sovereignty in the age of pandemics" (2020):[5]

"Digital sovereignty is about being able to control what we are doing. Not to do everything by ourselves or being completely independent. But to have the final say about what is ongoing here in order to maintain our regulatory sovereignty."

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A European strategy for data (2020):[6]

"The functioning of the European data space will depend on the capacity of the EU to invest in next-generation technologies and infrastructures as well as in digital competences like data literacy. This in turn will increase Europe's technological sovereignty in key enabling technologies and infrastructures for the data economy."

---

4 State of the Union Address by President von der Leyen at the European Parliament Plenary, 16 September 2020, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655.

5 Debate with Margrethe Vestager: Digital sovereignty in the age of pandemics, 24 April 2020, https://cerre.net/news/debate-with-margrethe-vestager-digital-sovereignty-in-the-age-of-pandemics/.

6 European Commission, COM(2020)66 final, 19 February 2020, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A European strategy for data.

Thierry Breton, European Commissioner for Internal Market, Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence:[7]

"Our society is generating a huge wave of industrial and public data, which will transform the way we produce, consume and live. I want European businesses and our many SMEs to access this data and create value for Europeans – including by developing Artificial Intelligence applications. Europe has everything it takes to lead the 'big data' race, and preserve its technological sovereignty, industrial leadership and economic competitiveness to the benefit of European consumers."

"*[Technological sovereignty] is not a protectionist concept, it is simply about having European technological alternatives in vital areas where we are currently dependent.*"

Guillaume Poupard, French Director General of French National Security Agency ANSSI:[8]

"The year 2020 marks the beginning of a new European cycle. Europe must be able to assert its sovereignty in the cyber field in order to promote its values of peace and stability in cyberspace at the international level"

Germany – The Digital Sovereignty Focus Group (Ministry for Economic Affairs) for the Digital Summit in 2019: [9]

"The digital sovereignty of a state or an organisation inevitably consists of the complete control over stored and processed data and the autonomous decision on who is allowed to access it. This also includes the capability of independently developing, altering and controlling technical components and systems, and supplementing them with other components."

Peter Altmaier, German Minister for Economic Affairs, Speech at the Digital Summit 2019:[10]

"Data are becoming the most important raw material of the future. The European economy urgently needs an infrastructure that ensures data sovereignty and broad availability of data whilst providing high security standards."

---

7 European Commission, 19 February 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273.

8 12th edition of the International Cybersecurity Forum, 28-30 January 2020, Lille, France, https://www.ssi.gouv.fr/en/actualite/fic-2020-anssi-calls-for-european-sovereignty-in-cybersecurity/.

9 Federal Ministry for Economic Affairs and Energy, The Digital Focus Group of the Innovative Digitisation of the Economy Platform for the 2019 Digital Summit, from 30 November to 1 December 2019, Page 6, paragraph 2.2.

10 Speech of Minister Altmaier during the 2019 Digital Summit, Dortmund, 29 October 2019, https://www.de.digital/DIGITAL/Redaktion/EN/Meldungen/2019/20191028-altmaier-we-need-our-own-european-data-infrastructure.html.

Anja Karliczek, German Minister for Education and Research, Digital Summit 2019:[11]

"*…with Gaia-X - we require in Europe a Data sovereignty. That an infrastructure is made available with which we can work together."*

Peter Altmaier, German Minister for Economic Affairs, during a visit to San Francisco, 2019:[12]

"Germany has a right to digital sovereignty. Data clouds should not only be set up in the U.S. or China, but also in Germany so that European companies, which want secure and reliable data storage, have this option."

2.2 Categorising stated rationales and objectives of digital sovereignty

The quotes listed in the preceding section illustrate the variety of rationales and objectives attached to digital sovereignty as well as the similarity to terms like technological sovereignty which some policymakers use in the same context or even interchangeably.[13] In this section, we aim to categorise these quotes and derive a meaningful structure of themes attributed to digital sovereignty in order to develop a baseline conceptualisation that can be used and referred to throughout the present report.

The term digital sovereignty is used individually and collectively level at the national and European level. As regards the individual citizen, they point to the requirement that the right to privacy and self-determination over what happens with personal (digital) data must be safeguarded. As regards the collective level, the quotes allude to the necessity of control over data and information in the digital space, the capacity to reap the economic benefits of that data as well as to participate in world-leading R&D. Furthermore, at the collective level, it is about being able to make autonomous decisions and having resilient infrastructures, in particular regarding critical infrastructure.[14]

---

11 Anja Karliczek, German Minister for Education and Research, Digital Summit 2019, Dortmund 29 October 2019, https://hpi-digitalblog.de/interview_post/anja-karliczek-ueber-ki-oekosystem-digitalgipfel-2019-hpi-digitalblog/.

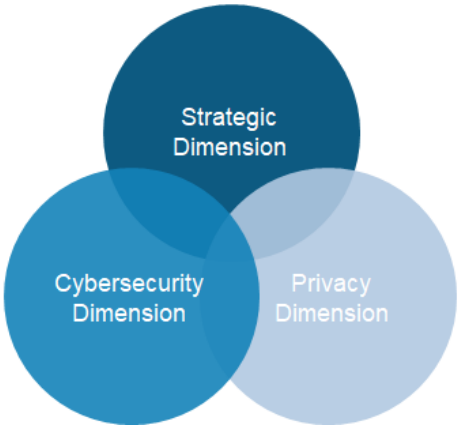
12 Peter Altmeier visiting San Francisco, 9 July 2019, https://www.bloomberg.com/news/articles/2019-07-09/germany-makes-push-for-cloud-service-independent-of-u-s.

13 For a discussion see also Bauer, M. and Erixon, F. (2020): "Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls", ECIPE Occasional Paper 02/2020, https://ecipe.org/wp-content/uploads/2020/05/ECI_20_OccPaper_02_2020_Technology_LY02.pdf. Eckert (2020) arrives at a similar conclusion and describes digital sovereignty as a "fuzzy concept". See https://fipra.com/update/dissecting-euco-buzzwords-european-digital-sovereignty-tech-independence-strategic-autonomy/.

14 On the one hand, an increased reliance on digitisation and interconnectedness of critical (national) as well as industrial infrastructures offers substantial benefits as regards their efficiency as well as enabling new business models. On the other hand, new opportunities for adversaries emerge. For a discussion, see e.g. Dickinson, B., & Wilkinson, D. (2019): Securing industrial systems in a digital world. The APPEA Journal 59(2): 574-577. and Emanuilov, I. 92019): International (Cyber)security of the Global Aviation Critical Infrastructure as a Community Interest. In Vedder, A. et al. (Eds.): Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security. Vol. 7: 299-342.

Abstracting from the specific themes emerging from the quotes, we identify three broad dimensions of digital sovereignty; (1) a privacy dimension at individual level, (2) a cybersecurity dimension at national and European level; and (3) a strategic dimension at national and European level where it is about maintaining the national sovereignty and having European alternatives in key technologies.

Figure 2-1: Three dimensions of digital sovereignty



Source: WIK-Consult.

These three dimensions reflect the central issues permeating the academic (and partly public) debate around how the availability of digital data, computing power and computer networks has impacted states' sovereignty and individuals' privacy. In fact, this debate is almost as old as computers and computer networks themselves.[15] Recently, in line with the general "geopolitical" stance of the von der Leyen Commission, the public debate around digital sovereignty has taken a turn to emphasise the strategic dimension subsuming both cybersecurity and privacy under the banner of sustaining a European alternative to its economic and ideological rivals, i.e. China and the US. The following Chapter analyses the broader European context of digital sovereignty in detail.

15 For an early example discussing all three dimensions, see Steinmüller, W. (1979). Legal problems of computer networks: A methodological survey. Computer Networks (1976), 3(3), 187-198. The debate received increased attention during the 1990s when the internet became popular with consumers and its ability to fundamentally change our way of life started to become visible. See, for instance, Perritt Jr, H. H. (1997). The Internet as a Threat to Sovereignty-Thoughts on the Internet's Role in Strengthening National and Global Governance. Ind. J. Global Legal Stud., 5, 423-442. or Sassen, S. (1997). On the Internet and sovereignty. Ind. J. Global Legal Stud., 5, 545-559.

3 The European Context on Digital Sovereignty

In this chapter, we set out to describe the broad context of digital sovereignty reflected in the strategy announced by the von der Leyen Commission, emphasised by the COVID-19 pandemic, which highlighted some critical dependencies on non-EU countries. We furthermore discuss how the pillars of the Digital Single Market (DSM) pertain to digital sovereignty.

3.1 A "geopolitical Commission"

As pointed out in the introduction of this report, the EU and its Member States are facing an increasingly complex situation in international relations. The EU will have to adapt to this situation and retain a voice of its own if it does not want to put its ability to act autonomously at risk.

The von der Leyen Commission recognised this from the outset. In her first press conference when taking over the role as the President of the European Commission from Jean-Claude Juncker, Ursula von der Leyen made clear that she will lead a "geopolitical Commission".[16] The political guidelines she set related closely to the topic of digital sovereignty as she pointed out that "...*it is not too late to achieve technological sovereignty...*" referring to areas including block chain, high-performance computing, quantum computing, algorithms and tools allowing data sharing and data (re-)use.[17]

Similarly, the Commissioner for the Internal Market, Thierry Breton, argued for a Euro-centric technology agenda insisting that "*...this is not a protectionist concept, it is simply about having European technological alternatives in vital areas where we are currently dependent.*"[18]

A recent paper published by European Parliamentary Research Service (EPRS)[19] draws the link between strategic autonomy and digital sovereignty as it underscores "digital dependence on the USA and China" (p. 48) as the trigger for heightened attention of EU policymakers on gaining digital sovereignty. The stance towards reducing this technological (digital) dependency is reflected in various policy initiatives launched by the Commission. To (re-)gain control over data appears to be at the centre of the EU's interests within its stance towards digital sovereignty. First and foremost, the European Commission recognises that data is at the centre of the digital transformation and therefore the most fundamental and important building block for the long-term

16 See Bayer, L. (2019): Meet von der Leyen's 'geopolitical Commission'. Politico. Online article: https://www.politico.eu/article/meet-ursula-von-der-leyen-geopolitical-commission/.

17 https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf, page 13.

18 https://ec.europa.eu/commission/commissioners/sites/comm-cwt2019/files/commissioner_ep_hearings/answers-ep-questionnaire-breton.pdf, page 3.

19 See EPRS (2020): On the path to 'strategic autonomy' – The EU in an evolving geopolitical environment. European Parliamentary Research Service. PE 652.096.

economic growth in Europe as well as the short-term recovery from the pandemic. Among other documents, the recently published draft Data Governance Act[20] reflects this understanding. This recognition comes at a time when US companies dominate the cloud market in the EU and through online platforms fuelled by online advertising (e.g. social media) have unrivalled access to EU citizens personal data.[21]

Accordingly, one of the first policy initiatives echoing this push towards the provision of digital tools originating in the EU, that emerged from the Von der Leyen Commission, was the plan to create a "single European data space". This concept refers to an EU-designed single market for data that shall enable companies (and in particular SMEs) across the EU to reap the benefits from data which would otherwise be difficult or impossible for them to access. The European Strategy for Data Communication[22] outlines the concept in detail while Thierry Breton summarises its goal as follows[23] "...*European data will be used for European companies in priority, for us to create value in Europe*."

A central initiative is the Franco-German project GAIA-X, also dubbed "AI-Airbus". GAIA-X aims to establish a common data infrastructure based on European values. Specifically, the German Federal Ministry for Economic Affairs understands "…*data infrastructure as a federated technical infrastructure, consisting of components and services that make it possible to access data and to store, exchange and use it according to predefined rules. We understand a digital ecosystem as the network of developers, providers and users of digital products and services, connected with transparency, wide-based access and a vibrant process of interchange. Such a system thus serves as a crucial foundation for European growth, digital innovations and new business models.*"[24] The central contribution of GAIA-X is a shared 'architecture' for data storage and sharing. "*The architecture employs digital processes and information technology to facilitate the interconnection between all participants in the European digital economy. By leveraging existing standards, open technology and concepts, it enables open, consistent, quality-assured and easy-to-use innovative data exchange*

20 See COM(2020) 767 final.

21 For an overview of the market position in cloud data storage see Table 4-1 in this report. The dominance of a small number of large (gatekeeper) platforms is reflected in the European Commission inception impact assessment for the ongoing legislative procedure of the Digital Services Act. See European Commission (2020): Digital Services Act package: Ex ante regulatory instrument for large online platforms with significant network effects acting as gate-keepers in the European Union's internal market. Ref. Ares(2020)2877647 - 04/06/2020. The majority of the small number of these gatekeeper platforms originate in the US (rather than the EU).

22 European Commission (2020): A European strategy for data. COM(2020) 66 final.

23 https://audiovisual.ec.europa.eu/en/video/I-183075.

24 Quoted from Federal Ministry for Economic Affairs and Energy, & Federal Ministry of Education and Research (n.d.): Project GAIA-X - A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem. Executive Summary. Available at: https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/das-projekt-gaia-x-executive-summary.pdf?__blob=publicationFile&v=6.

and services. Additionally, GAIA-X will become a facilitator for interoperability and interconnection between its participants for data as well as services."[25]

As an application for the enabled improvement in data (re-)use and sharing, the Commission points to artificial intelligence (AI) as a key capability for the EU and its Member States going forward. In line with the strategic dimension of digital sovereignty, the Commission's goal is to enable cutting edge research around AI and its application, and reaping the economic potential that it brings. To this end, the Commission aims to unify the approach towards AI based on European values, norms and ethics across Member States of which many have already launched their own individual AI strategies.[26]

Another example of current policy initiatives of the Commission aligned with the strategic dimension of digital sovereignty is the European High Performance Computing Joint Undertaking (Euro HPC JU).[27] It represents a legal and funding instrument focused on establishing a pan-European supercomputing infrastructure that may be used in scientific and industrial application fields, including but not limited to developing AI applications. The Euro HPC JU aims to build HPCs within the EU alleviating the existing dependency on non-EU computing power.[28] This Joint Undertaking will have a budget of around 1 billion euros with additional resources provided by private entities.[29]

The topic featuring most prominently in the public debate around digital sovereignty is without a doubt the imminent rollout of 5G technology across the Member States of the EU and the UK. On 22 March 2019, the European Council called for a coordinated approach to the cybersecurity of 5G networks as it noted that 5G networks have more

---

25 Quoted from GAIA-X (2020): GAIA-X Technical Architecture. Available at: https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-technical-architecture.pdf?__blob=publicationFile&v=5.
Notably, an analysis by the New Zealand Embassy clarifies that "GAIA-X will not be a European cloud provider or cloud service to store and share data online per se. Equally it does not seek to connect a network of servers and computers around the world with big data computing capacity and data storage. Instead, GAIA-X can best be understood as a meta-level project that seeks to link existing (and newly created) clouds together in a network, so that data silos from different economic sectors and different companies in Europe are connected and made accessible to other users. By setting standards and facilitating interoperability, GAIA-X aims to connect all these different data infrastructures and bring many solutions into a homogeneous, user-friendly system." Quoted from New Zealand – Foreign Affairs and Trade (2020): Gaia-X – A European Cloud Infrastructure and Data Ecosystem. Market Report. Available at: https://www.mfat.govt.nz/assets/Trade-General/Trade-Market-reports/Gaia-X-A-European-Cloud-Infrastructure-and-Data-Ecosystem-20-August-2020-PDF.pdf.

26 The White Paper on AI recently published by the European Commission reflects this and proposes a process to ensure that AI applications adhere to European values and norms. See https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

27 See https://eurohpc-ju.europa.eu/ Notably, while the HPC facilities themselves may alleviate the dependency of EU-based enterprises and researchers on non-EU HPC computing power, the vendors selected for projects under the initiative include also non-EU vendors such as Hewlett-Packard Enterprise for a significant number of facilities announced so far.

28 The European Commission pointed out that currently European industry only provides around 5 percent of supercomputing resources while consuming around 30 percent of these resources, hence clearly implying dependencies on competitors in the US, China and Japan.

29 https://eurohpc-ju.europa.eu/.

pronounced security risks compared with existing network generations.[30] Hence, Member States must complete national risk assessments and coordinate at European level for which a so called toolbox has been made available. The resulting debate revolves mainly around which suppliers will be allowed to provide the infrastructure required for updating the respective mobile networks. In particular, Huawei and ZTE – the Chinese competitors of the European suppliers Ericsson and Nokia – have drawn the attention of policymakers and regulators throughout the EU as well as in the UK. Various countries have decided to (partly) exclude Huawei and ZTE from 5G rollout or have set limits for their involvement.[31]

These initiatives on the EU-level exemplify the Commission's objective of (re-)gaining strategic autonomy as regards key digital technologies. The COVID-19 pandemic has further highlighted the dependency of European governments and businesses on non-EU providers of technology. We focus on this aspect in the next section.

3.2 COVID-19 – A spotlight on existing dependencies

According to a report from the European Parliamentary Research Service (EPRS)[32], the COVID-19 crisis has disturbed global supply chains and shed light on existing dependencies on other countries, in particular China. Specifically, the scarcity of medical equipment during the first weeks of the crisis took many political leaders by surprise resulting in a recurrence of individual states' individualistic reflexes. Furthermore, EPRS stated that only as the crisis progressed was the Commission able to reunite Member States under the banner of a common strategic autonomy – a central theme of the recovery process from the economic damage of the pandemic.

Amid lockdowns across Europe, there was a step-change in the adoption of digital solutions. In many sectors, digital processes were implemented swiftly to enable at least part of the work processes to continue. Practices widely adopted include video-conferencing, online education, home office, video appointments with doctors and more. According to DE-CIX, one of the world's leading internet exchanges in Frankfurt, Germany, the number of video-conferences has increased by 100% compared with the period before COVID-19.[33] Microsoft indicated that its Teams platform and Cloud services have increased by 775% while other platforms such as Zoom and Slack

30 Via EU Recommendation 2019/534, see also https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_1833.

31 The publicly stated rationale behind such (partial) bans of non-EU suppliers refers to cybersecurity concerns. The underlying rationale however appears to be much more driven by geopolitics and essentially strategic concerns as Rühlig & Björk (2020) suggest. See Rühlig, T. & Björk, M. (2020): What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe. Stockholm: The Swedish Institute of International Affairs.

32 See EPRS (2020): On the path to 'strategic autonomy' – The EU in an evolving geopolitical environment. European Parliamentary Research Service. PE 652.096.

33 See https://www.de-cix.net/de/news-events/news/internet-usage-continues-to-surge.

mention record increases over the same period. [34] Notably, a few EU-based collaboration software companies benefitted from the pandemic in a similar manner with TeamViewer as a notable exception.[35]

Furthermore, due to the temporary closures of 'brick and mortar' shops, there has been an accelerated shift towards online businesses and in particular e-commerce offerings. As even the most reluctant customers become accustomed to online shopping, it might well be that after the crisis, these trends towards digital commerce may persist. Although there are various EU- and UK-based e-retailers, marketplaces and platforms such as Allegro (Poland), Fnac (France), Otto Group (Germany), or Zalando (Germany), they experience strong competition from globally successful players such as Alibaba (China), Amazon (US), Ebay (US), Google Shopping (US), Facebook Marketplace (US), or JD (China).

Furthermore, it became clear that tracing applications installed on smartphones can be one part of the governmental strategy to contain the virus. These applications use sophisticated sensors featured on modern smartphones to produce a social graph of potentially risky encounters with people who were later tested positive. Thus, those who came in contact with infected and potentially contagious others can self-isolate. The debate that followed revolved around the justified interest of mass movement tracing versus data privacy now and in the future, and also the dependence on the cooperation of Apple and Google.[36]

These are only a few obvious examples of how digital services and ultimately digital infrastructures will gain further importance as people and businesses, including government institutions, rely on them more intensively during the pandemic and quite likely also thereafter.

Finally, the stance towards an increased strategic autonomy emerging from the pandemic reflected in Ursula von der Leyen's announcement of the €750 billion recovery fund which shall "*...repair our social fabric, protect the single market and rebalance company balance sheets across Europe*." In addition, she mentioned that this fund would also "*...allow investment in new infrastructure such as 5G…*" and will make Europe "*…more resilient for future crises…*".[37]

---

34 See https://www.zeit.de/digital/2020-03/videokonferenzen-zoom-app-homeoffice-quarantaene-coronavirus.

35 TeamViewer is a German software provider headquartered in Goeppingen (close to Stuttgart), see www.teamviewer.com (Notably, a majority stake in the company is being held by a private equity firm based in London and therefore outside of the EU.).

36 Apple and Google have an effective duopoly of smartphone operating systems, which led to challenges for many governments in EU Members State who wanted to promote their own corona tracing applications. Apple and Google were required to provide access to user data, which conflicted in some instances on their compliance with the EU GDPR.

37 The European parliament, 28 May 2020, https://www.theparliamentmagazine.eu/articles/news/european-commission-unveils-%E2%82%AC750bn-coronavirus-recovery-fund.

However, as the following section elaborates, this stance towards strategic autonomy already transpires from various initiatives under the Digital Single Market predating the von der Leyen Commission as well as the pandemic.

3.3 The Digital Single Market strategy and Digital Sovereignty

Although not directly considered a 'digital sovereignty strategy', the Digital Single Market (DSM) of the previous Commission already reflected some of the dimensions of digital sovereignty identified in the preceding Section 2.2.

The fundamental idea of the DSM is to create a single market across all Member States of the EU, in which the free movement of goods, persons, services and capital is ensured. With this, individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition. Furthermore, a high level of consumer and personal data protection in line with European values is guaranteed, irrespective of nationality or place of residence.

The DSM builds on three pillars; *Access* (better access to digital goods and services), *Environment* (the right conditions and a level playing field for digital networks to grow) and *Economy & Society* (maximising the growth potential of the digital economy). Thus far, 28 legislative initiatives, which were originally presented by the previous (Juncker) Commission, have been politically agreed or finalised by the Parliament and the Council. Some of these initiatives aim to benefit the digital services and sector in general, like investments in public Wi-Fi hotspots, the abolition of roaming charges and having access to online subscription materials (e.g. video on demand, etc.) when travelling within the EU and efforts to counter disinformation.

Other initiatives can be interpreted as fostering digital sovereignty along two of the three dimensions which we identified before; mainly the cybersecurity and the strategic dimensions.

Regarding the **cybersecurity dimension**:

- The European Union Agency for Network and Information Security (ENISA) published guidance on the identification of Critical Information Infrastructure (CII), assets and services.[38] These documents were specifically targeted at Member States that were at the beginning of CII protection structure development or were looking to further improve existing structures.

38 Council Directive 2008/114/EC and . Stocktaking, Analysis and Recommendations on the protection of CIIs. See respectively http://data.europa.eu/eli/dir/2008/114/oj and https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis.

- In August 2016, the Directive on security of network and information systems[39] entered into force. Besides providing the legal base, the EU will also create a network of European centres of cybersecurity expertise, in order to reinforce these capacities in the EU.. Cybersecurity, which combines digital capabilities with national sovereignty, can also be interpreted as an effort towards digital sovereignty.

Regarding the **strategic dimension**:

- The European Commission also launched strategies and investments regarding artificial intelligence and robotics to boost the EU's research and industrial capacity as these technologies are considered key drivers of future innovation and economic growth. The European wide approach is to ensure that Europe remains at the forefront of these technologies while ensuring that European values are respected.
- Furthermore, the Euro High Performance Computing Joint Undertaking was established in 2018 aiming to equip Europe with a world-class supercomputing infrastructure, which will support leading R&D in many sectors.[40]

The abovementioned initiatives contribute towards the overarching objective of the DSM strategy for Europe to maintain its position as a world leader in the digital economy and help European companies to grow globally.[41] The DSM in retrospect reflects what can be viewed today as the strategic dimension of digital sovereignty.

39 See http://data.europa.eu/eli/dir/2016/1148/oj.

40 The European Commission, 2015: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Single Market Strategy for Europe, {SWD(2015) 100 final}. See also the factsheet: A Digital Single Market for the benefit of all Europeans, https://ec.europa.eu/commission/sites/beta-political/files/euco-sibiu-a_digital_single_market.pdf.

41 The European Commission, 2015: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Single Market Strategy for Europe, {SWD(2015) 100 final}.

4 Digital Sovereignty across the EU and the UK

In this chapter, we describe key results from our review of the policy initiatives in the 27 EU Member States and the UK, that can be interpreted as contributing to digital sovereignty. First, we present the main findings of our research. We focus on the two dimensions of digital sovereignty that contribute to the EU's strategic autonomy objective, i.e. the strategic dimension and the cybersecurity dimension. The last section of this chapter summarises the detailed individual country fiches in the Annex.

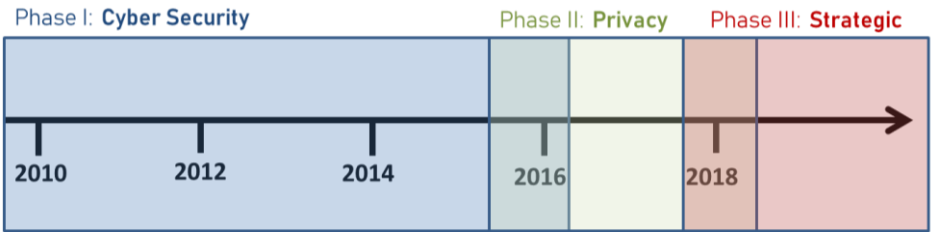
It should be noted that virtually all European Member States have recognised the importance and the impact that digital transformation brings to their citizens, businesses and governments. Their digital agendas, strategies and so forth bear witness to that in laying out ambitious plans to upgrade infrastructure, skills and digitalisation across the board. While such measures may lay the groundwork for digital sovereignty, this report does not aim to analyse or even evaluate the individual digital strategies unless they actually emphasise digital sovereignty or strategic autonomy in some specific way. Consequently, the results presented in the following sections focus closely on the dimensions developed in Section 2.2 and the aspects mentioned by key policymakers and EU officials as described in Section 2.1.

4.1 Varied scope of applied Digital Sovereignty

We find that the initiatives adopted in the individual states differ substantially regarding the dimensions of digital sovereignty they address. However, it has emerged that countries with established policy initiatives addressing the strategic dimension inevitably also address the other two dimensions of cybersecurity and privacy. Furthermore, we found that all of the countries analysed as part of this report feature specific policy measures addressing the cybersecurity dimension of digital sovereignty. On this subject, the collected data show that policymakers and regulators in the reviewed countries follow a progressive approach from a 'narrow' interpretation of digital sovereignty merely covering cybersecurity to a 'broad' understanding of the concept also featuring the privacy and strategic dimensions of digital sovereignty, as identified in Section 2.2.

This seems to align with the development of the different dimensions of digital sovereignty over time, based on the moment when the different measures were launched in Europe, as depicted in following graph.

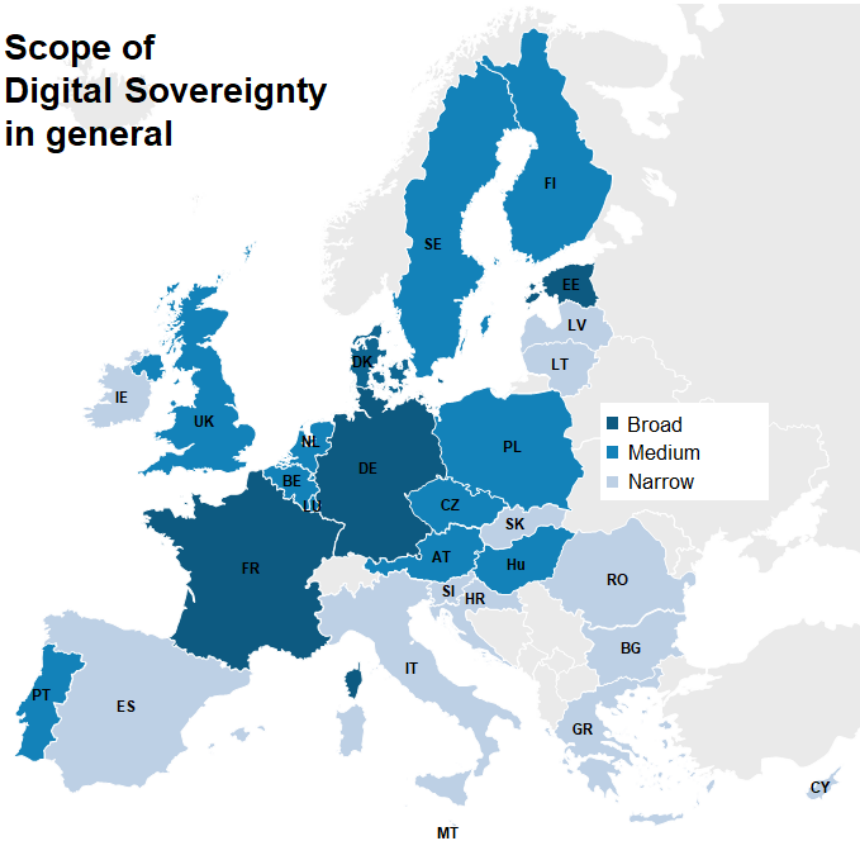
Figure 4-1: Developing dimensions of digital sovereignty over time



Source: WIK-Consult.

The figure below summarises our findings on the dimensions addressed in the analysed countries.

Figure 4-2: Scope of digital sovereignty (cybersecurity/ privacy/strategic)



Source: WIK-Consult.

It shows that the scope of digital sovereignty in the individual Member States differs greatly. Thus, in about half of European countries, there is a rather narrow interpretation of digital sovereignty prevails (coloured light blue). This means that in these states digital sovereignty does not include any components or aspects beyond cybersecurity measures.

The states with a medium scope of digital sovereignty (coloured normal blue) have the cybersecurity dimension supplemented with the privacy dimension of digital sovereignty. The topic of digital sovereignty has already led to complementary measures in these states, but they are usually of a more reactive nature, i.e. they are focused on the defence against cyber-attacks and espionage.

In states with a broad scope of digital sovereignty (coloured dark blue), the question of digital sovereignty has been raised across a broad selection of, if not all, sectors of the economy. In these Member States the public debate and the corresponding (planned) measures stretch beyond the economic impact as digital sovereignty is viewed as a prerequisite for nation-state sovereignty and sustaining national and European core values. The countries following such a broad strategic understanding of digital sovereignty are France, Germany, Denmark and Estonia.

It is worth noting that an explicit digital sovereignty strategy only exists at the EU-level, and in Germany and France. Thus far, the considerations on digital sovereignty have either been incorporated into the countries' general digitisation strategies or are being integrated into the national cybersecurity strategy. However, it seems, it will only be a matter of time before more explicit digital sovereignty strategies are adopted given the newly emphasis on strategic autonomy.

Against this backdrop, the following sections present detailed analyses of the two dimensions of digital sovereignty that contribute to strategic autonomy. We begin with the strategic dimension and then focus on the cybersecurity dimension.

4.2 The strategic dimension of Digital Sovereignty across Europe

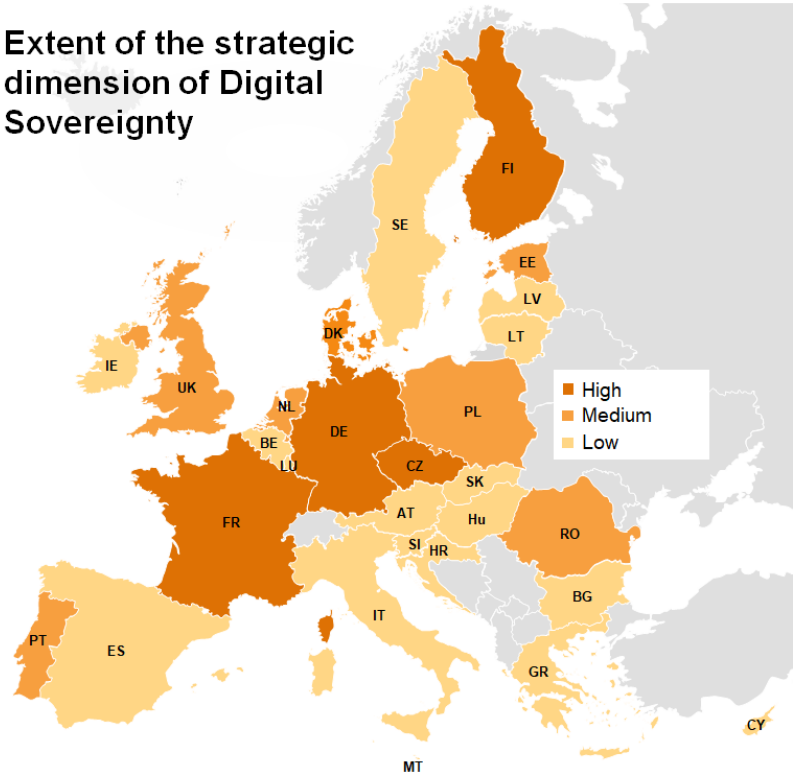
4.2.1 Differences in the extent of strategic actions as regards digital sovereignty

As noted previously, the strategic aspects of digital sovereignty are most pronounced in France and Germany. The strategy papers of both countries state that digital sovereignty also concerns defending European values such as freedom, solidarity and tolerance. This value-based argument leads to an proactive approach to achieve digital sovereignty. It is not enough for the systems to be secure (cybersecurity dimension) and for data protection to be guaranteed (privacy dimension), but independence from non-European providers must be achieved (by using European alternatives, for example, in AI it is ensured that European values are respected).

As can be seen from Figure 4-3, the Member States differ the most in the scope of the strategic dimension of digital sovereignty:

- When a country is marked dark brown as having a “High” extent of the strategic dimension of digital sovereignty, it means that the respective country is taking or planning extensive strategic and economic policy measures to increase its independence from non-EU providers[42] in the digital economy. In this context, strategic autonomy is defined nationally or EU-wide.
- Countries marked medium brown as “Medium” have interpreted digital sovereignty strategically and have also taken measures in this direction, but not comprehensively and to a lesser extent than countries with the "high extent" label.
- Countries marked light brown as “Low” hardly interpret digital sovereignty within the strategic dimension, if at all. This does not mean that these countries do not address the issue of digital sovereignty at all. For example, extensive cybersecurity measures could still have been taken in the context of digital sovereignty. However, in these countries it is not apparent whether measures were taken in view of geostrategic or geopolitical considerations.

Figure 4-3: Extent of the strategic dimension of Digital Sovereignty (high-low)



Source: WIK-Consult.

42 Foreign providers in the case of the UK.

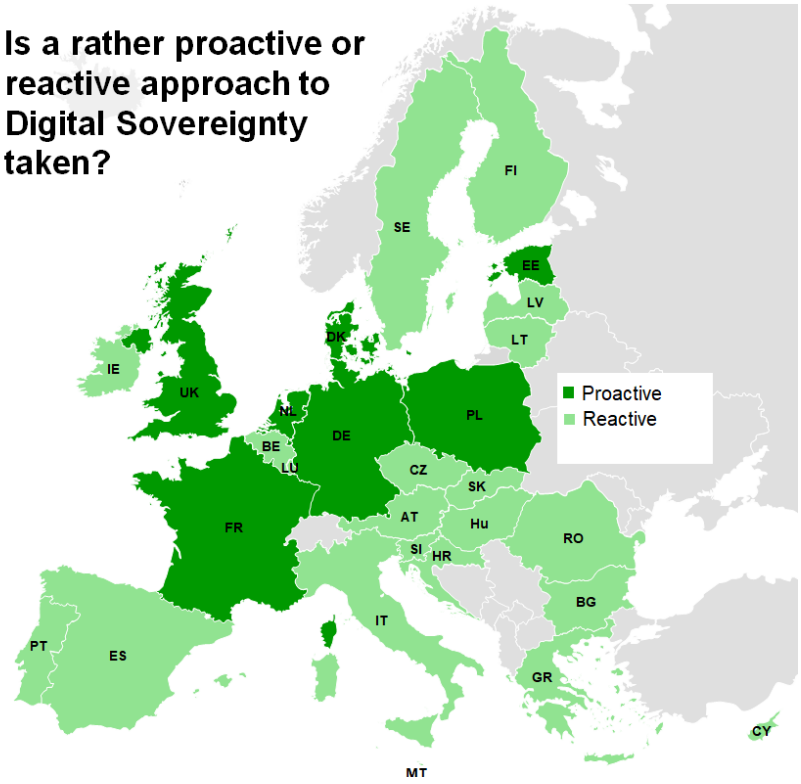
It is noticeable that the larger Member States, such as Germany and France, address the strategic dimension in particular. The larger Member States also tend to take a more proactive approach to achieving digital sovereignty than the smaller states, as shown in Figure 4-4. “Proactive approach" in this context means that extensive economic policy or geostrategic measures are taken to reduce dependency on foreign providers (examples include the exclusion of certain providers of infrastructure and services and the establishment of data embassies,[43] etc.). In contrast, a “reactive” approach is characterised by adopting a reactive stance against attacks. These countries primarily try to take protective measures and refrain from economic policy measures with a high degree of intervention.

Denmark is an exception. As a smaller country, it has nevertheless taken a proactive approach by launching the “TechPlomacy” initiative. Denmark is the first country in the world to have an official Tech Ambassador with locations in Silicon Valley and Beijing. The role of the Tech Ambassador is to represent Denmark’s interests vis-à-vis the large digital companies considering their influence in the digital area.

Another small country with a rather proactive approach to digital sovereignty is Estonia. Estonia is the European leader in the digitisation of public administration. Accordingly, in Estonia, national sovereignty is more closely linked to digital sovereignty than in other countries, as cyber-attacks can simultaneously attack the core functions of the government. Estonia was the first country in the world to create so-called “data embassies” abroad. These data servers are located abroad, while still under the sovereignty of Estonia in the same manner as official embassies. The aim of this approach is to increase independence through the decentralisation of stored data and thus contribute to digital sovereignty.

43 Data embassy is a concept where a country owns server resources outside its borders, while still falling under its own jurisdiction (like a normal embassy). These resources will not only be used for data backup, but also for operating critical services. Luxembourg has started with this concept for Estonia.

Figure 4-4: Proactive or reactive approach to digital sovereignty



Source: WIK-Consult.

4.2.2 Different positions towards non-European companies

There are also differences between countries in their attitude towards non-European companies. While there seems to be broad agreement that Chinese suppliers should be screened and partly restricted regarding the provision of critical parts for the 5G infrastructure (see Section 4.3), the approach towards US companies differs. There are countries like the UK, Ireland, Estonia, and Romania with a softer attitude towards US companies versus countries like France and Germany that have a more restrictive approach focussing on increasing the competitive position of national and European suppliers in key technologies.

On the 'softer' side, in particular, the UK sees its withdrawal from the European Union as an opportunity to establish itself as an attractive European location for US suppliers. The UK's latest plans to completely ban Huawei as a 5G supplier align with the American position.[44] This also applies to Ireland, which interprets digital sovereignty

44 The UK has restricted the use of technology supplied by Huawei to its Radio Access Network and in addition restricted this to 35%. This regulation could be tightened further as plans were announced in October 2020 to set a complete phase out date of Huawei by 2027. See https://www.theguardian.com/technology/2020/may/22/boris-johnson-forced-to-reduce-huaweis-role-in-uks-5g-networks and See https://telecoms.com/506844/uk-mps-recommend-faster-huawei-removal-if-china-doesnt-behave-itself/.

narrowly and takes a reactive approach, focusing on the security of its ICT infrastructure.[45] The motivation behind Ireland's position might be that many US tech companies are currently based in Ireland, and should not be frightened off by restrictive measures.

Furthermore, there are European countries that have extensive collaboration with the US government in areas surrounding digital sovereignty; e.g. Estonia and Romania collaborate with the US on data centres and even cybersecurity. Several EU Member States also cooperate with the US regarding selection criteria for 5G suppliers (EE, CZ, SI, RO, PL, and LV). In Eastern Europe, the increasing geopolitical importance of digital sovereignty is becoming more apparent. Above all, countries that for historical and/or strategic reasons want to protect themselves from stronger Russian influence (such as PL and EE) tend to maintain closer cooperation with the US on ICT security issues. The US, has an interest in gathering support in Europe for its position versus Chinese 5G suppliers as well as defending its other interests in the digital area.

In light of the traditional strong ties between European states and the US, it appears that there is less reluctance to accept dependence on US-based companies and/or technology than to accept a potential dependence on non-European suppliers or technology from other regions of the world.

As a matter of fact, hardware independent from the specific manufacturer's headquarter location will (most probably) has been produced with inputs from a complex global supply chain featuring material and technological inputs from many countries other than the one where the headquarters happen to be located. Likewise, software typically draws on a variety of inputs which will likely not be limited to a specific territory. Against this backdrop, the apparent selection strategy of vendors under the banner of digital sovereignty may be questionable. To achieve digital sovereignty for the EU in line with the idea propagated by top EU officials (see Section n 2.1) would likely entail a rigid inspection of hardware and software independent of the country of origin of the respective manufacturer as well as building capability within the EU to develop home-grown digital champions. Notably, these digital champions would equally have to comply with rigid testing regimes for hard- and software.

To put this in the right context, we refer back to the earlier quotes from European policy makers (see Section 2.1), that digital sovereignty is not "*…to do everything by ourselves or being completely independent. But to have the final say about what is ongoing here in order to maintain our regulatory sovereignty." (*Margarethe Vestager), and it "*…is not a protectionist concept, it is simply about having European technological alternatives in vital areas where we are currently dependent.*" (Thierry Breton).

45 Incumbent EIR restricted Huawei to its Radio Access Network but continuous its working relation with Huawei. In addition, no restriction for government to work with non EU cloud services apart from top secret documents. See https://www.irishtimes.com/business/technology/eir-very-happy-with-huawei-as-supplier-for-5g-network-1.4153946.

4.2.3 Control of non-European investments in crucial infrastructure

Our desk research revealed that capping or introducing increased review measures on foreign direct investments (FDI) in (critical) infrastructure or specific industries can equally be employed as a tool to curb the influence of non-national, non-EU or non-European companies. Above and beyond the debate around the European FDI Screening Regulation which took effect in October 2020,[46] this kind of tool seems to have gained traction during the COVID-19 crisis as some European companies have decreased significantly in value or are in need of cash, which makes them vulnerable to take-overs or capital investments from foreign-owned companies.

The Commission further noted, that should an FDI not go through a national screening process, such FDI could be subject to ex post review by the Commission up to 15 months after completion of the investment. European countries are currently obliged to provide notification of FDIs. In June 2020, a white paper was published by the European Commission setting out guidelines for legal instruments addressing the regulatory gap in relation to FDIs.[47]

Finland, Italy and Germany are examples of countries that have taken measures to control non-European investments and/or take-overs in companies related to crucial infrastructure. Beginning in 2020, the relevant Italian regulation was amended to cover not only critical infrastructure and technology but also security of supply and access to sensitive information. [48] Furthermore, the government of Austria is working on new FDI regulations, which will make it more difficult to take over Austrian companies in sectors ranging from AI and robotics, water and infrastructure, to food production.[49]

However, one needs to put this into perspective; capital investors (European and non-European) have played an important role in ICT infrastructure for the last 20 years as the ICT sector is capital intensive by nature and most companies in this sector are privately owned. Furthermore, due to the strong growth of the sector in the past 20 years and expectations for future growth, the sector is attractive to capital investors. Even if certain ICT initiatives are promoted at country level, e.g. the development of an AI industry, private capital will likely still be needed, especially in EU countries with a weaker economy. Coordination between Member States could be beneficial for digital sovereignty in Europe thereby clarifying which country could drive certain key technologies for the benefit of Europe as a whole. Furthermore, specific companies that play an important role in developing and maintaining these key technologies should be identified and subjected to (Europe wide) FDI regulation.

---

46 Regulation 2019/452 - In April 2019, the EU-wide framework for the screening of FDIs entered into force and will fully apply as of 11 October 2020. The aim of this Regulation is to create an EU-wide mechanism to coordinate the screening of FDIs, which are likely to affect the security and public order of Europe and its MS. At the moment 14 MS have national FDI screening mechanisms in place.

47 https://ec.europa.eu/competition/international/overview/foreign_subsidies_white_paper.pdf.

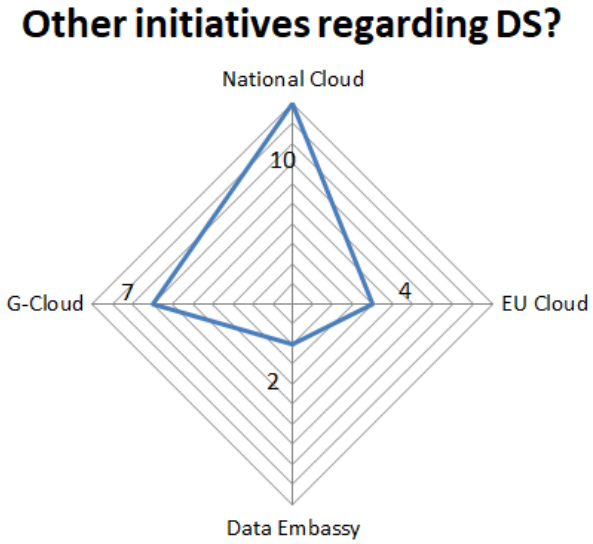
48 https://iclg.com/practice-areas/foreign-direct-investment-regimes-laws-and-regulations/italy.

49 https://www.sn.at/wirtschaft/oesterreich/neuer-anlauf-fuer-schutz-von-firmen-gegen-auslands-uebernahmen-86078275.

4.2.4 Cloud storage, cloud computing and data sovereignty

Alongside growing concerns about high risk vendors being in the supply chain for mobile networks, cloud storage and related infrastructure are also in the spotlight in many European countries. As shown in Figure 4-5, from the benchmark it appeared that the main focus is on cloud related initiatives supporting digital sovereignty (see below figure). The most attention has been given to national cloud initiatives, followed by Government clouds and European clouds. Other initiatives include data embassies, which enable a country to have (redundant) data centres abroad while formally still being under its national control. For example, the government of Estonia has such a data embassy located in Luxembourg.

Figure 4-5: Other initiatives to support Digital Sovereignty



Scale represents number of countries with an initiative in the respective category

Source: WIK-Consult.

The underlying concern and reason for the drive towards national and European cloud services and data centres under European control relates to (1) the potential dependency on non-EU and in particular US providers of cloud storage and (2) the potential infringement of data protection when data is stored with US-based providers of cloud storage due to the US Cloud Act.[50] US based cloud services have a large market share in Europe (see Table 4-1 below). This implies that a significant amount of data in Europe is subject to US law and can be accessed by the US intelligence services. The national and European cloud services, including the data embassy concept (which can be seen as an extension of cloud services), can be considered as European alternatives.

50 The US Cloud Act makes data held in the US or by American companies, subject to US Law no matter where the data is located. See https://www.congress.gov/bill/115th-congress/house-bill/4943.

Describing the market situation in more detail, Table 4-1 ranks the six largest cloud service providers in the major cloud markets in Europe (including IaaS, PaaS and hosted private cloud services). The ranking is done by revenue based on the first quarter of 2020. Overall, in Europe, the four largest players are US based firms.

Table 4-1: Rank of revenues of cloud service provider in Europe and selected EU countries, Q1 2020

Rank	Europe	UK	Germany	France	Netherlands	Rest of Europe*
1	AWS	AWS	AWS	AWS	AWS	AWS
2	Microsoft Azure	Microsoft Azure	Microsoft Azure	Microsoft Azure	Microsoft Azure	Microsoft Azure
3	Google Cloud	Google Cloud	Google Cloud	OVH	Google Cloud	Google Cloud
4	IBM	IBM	Deutsche Telekom	Orange	KPN	IBM
5	Salesforce	Rackspace	IBM	Google Cloud	IBM	Salesforce
6	Deutsche Telekom	Salesforce	Oracle	IBM	Oracle	Swisscom

Note: * Rest of Europe refers to the European countries excluding UK, DE, FR and NL. Source: Synergy Research Group.

There are, however, European alternatives offered by the telecommunication incumbents Orange, DT and KPN in their respective countries and by parties such as OVH and Salesforce. The four largest country markets (UK, DE, FR, and NL) account for 63% of the total European revenue (€5.3 billion in Q1 2020). This explains the drive for pushing European cloud initiatives like GAIA-X and related certifications demonstrating compliance with European values, regulation and security guidelines.

In this context, it is not surprising that governments in Germany and France are the strongest supporters of GAIA-X and that the Netherlands together with mainly Germany and Austria have developed recommendations for a cloud certification scheme. The explicit goal of GAIA-X is to form a data infrastructure that strengthens both the digital sovereignty of cloud service users and the scalability and competitiveness of European cloud service providers. The cloud certification would demonstrate compliance with European values, regulation and security guidelines and can strengthen the market position of European cloud services.

An alternative yet possibly compatible approach briefly touched on above is the Estonian concept of a data embassy. Estonia has implemented a “paperless governance policy” as part of their digitisation process. Its data are stored in a government cloud, which is physically hosted by (military grade secured) servers outside its borders, in this case, in Luxembourg. This is done to secure Estonia’s sensitive databases from natural disasters, but also from cyber, terrorist or military

attacks. As with physical Estonian embassies, the servers are considered sovereign embassies in foreign data centres. This implies that they fall under Estonian jurisdiction.[51]

Hence, a data embassy offers European countries a secure (military graded) redundant backup option in another European country, while still falling under their own (and European) jurisdiction. This could be a good back-up solution for other European countries as well.

It is also noted that US companies are investing in data centres across the European Union. Due to their relatively low energy prices and colder climates, the Nordic countries are partnering up with US Cloud providers Amazon, Google and Co, and partnerships have also emerged in the Netherlands, Romania and Luxembourg. It is unclear whether and how these partnerships impact the digital sovereignty in Europe, but it seems worthwhile reviewing them in the larger picture of European cloud services and European based infrastructure, and if a similar European approach is required.

Last but not least, the availability of European cloud services and European certification is meant to push the European Data marketplace. In line with the statements by EU officials provided in Section 2.1, data marketplaces can provide businesses in the EU, in particular SMEs, with access to data that they otherwise may not be able to use to their benefit. Looking forward, one major case for the use of external data is the development of AI applications. The next section sheds light on this aspect of digital sovereignty.

4.2.5 Artificial Intelligence

The Commission has recognised the central importance of artificial intelligence (AI) applications for innovation and future economic growth.

In February 2020, the Commission published its White Paper on AI together with its European Strategy for Data[52] with the aim of ensuring that Europe participates in the shaping of this key technology, synchronising the efforts among Member States and reaching a sufficient scale. [53]

Indeed, to be successful in AI Europe needs a data strategy since data is an essential input for the development of AI applications.

The White Paper on AI notes in this perspective: *"Harnessing the capacity of the EU to invest in next generation technologies and infrastructures, as well as in digital competences like data literacy, will increase Europe's technological sovereignty in key*

51 See https://www.oecd.org/gov/innovative-government/Estonia-case-study-UAE-report-2018.pdf.
52 See https://ec.europa.eu/commission/presscorner/detail/en/fs_20_283.
53 European Commission, COM(2020) 65 final, 19 February 2020, White paper on Artificial Intelligence - A European approach to excellence and trust. See https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

enabling technologies and infrastructures for the data economy. The infrastructures should support the creation of European data pools enabling trustworthy AI, e.g. AI based on European values and rules." Furthermore, this is about "…*to become a global leader in innovation in the data economy…"*

From the benchmark, it appears that all of the 27 MS plus the UK have or are currently working on an AI strategy. Some countries focus on stimulating AI based innovation and retaining talent thereby not missing out on economic opportunities (BE, DE, and PT), while other countries are more focused on security and militarily applications of AI (FR, IT, and UK).

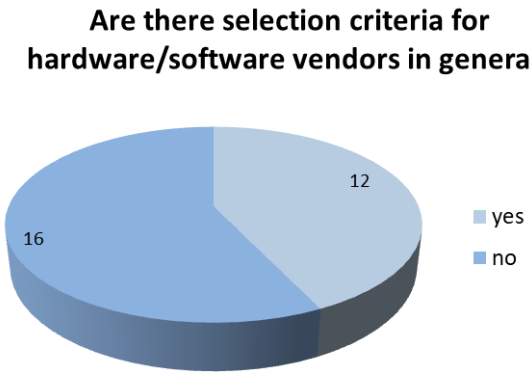
4.3 The cybersecurity dimension of digital sovereignty across Europe

The second dimension of digital sovereignty contributing strongly to strategic autonomy is cybersecurity. In this section, we review the policy initiatives and measures that are presented as increasing cybersecurity and resilience of digital infrastructure. Within the current public debate this dimension revolves around decisions about the specific providers selected to supply hardware and software for the rollout of broadband infrastructure covering both fixed and mobile networks. As we illustrated in Section 3.2, the increased reliance on digital tools during the pandemic has exacerbated already existing concerns. So has the geopolitical power play between the US and China and related accusations of state-funded cyber-espionage on both sides, which have further drawn the cyber security dimension of digital sovereignty into the spotlight.[54]

As shown in the figures below, the European benchmark shows that around 40% of EU countries have implemented selection criteria for hardware/software vendors in general. It is noteworthy that the Netherlands and Lithuania have proposed to elevate the debate of general selection criteria for ICT vendors to the European level (respectively for software and for having a blacklist on cybersecurity aspects for 5G suppliers and services).

54 Cyber-espionage can be carried out on the software or the hardware level. Examples are 'backdoors' in encryption machines, used by the CIA and BND or backdoors in Cisco routers and related "Lawful Access to Encrypted Data Act" introduced by US Senators. (see Brustolin, V., de Oliveira, D. & dos Reis Peron, A.E. (2020): Exploring the relationship between crypto AG and the CIA in the use of rigged encryption machines for espionage in Brazil. Cambridge Review of International Affairs. And Miller, G. (2020): 'The intelligence coup of the century' For decades, the CIA read the encrypted communications of allies and adversaries. Washington Post February 11, 2020.
For a literature overview how malware can be used by adversaries in conflicts and for espionage, see Easttom (2018): The Role of Weaponized Malware in Cyber Conflict and Espionage. In proceedings of ICCWS 2018 13th International Conference on Cyber Warfare and Security: 191-199. Furthermore,Hou and Wang (2020) describe various means of industrial espionage using digital means: Computers & Security 98 (November): 1-12. Lastly Alves and Morris (2018) focus on cyber-attacks relying on hardware: Hardware-based Cyber Threats. 4th International Conference on Information Systems Security and Privacy.

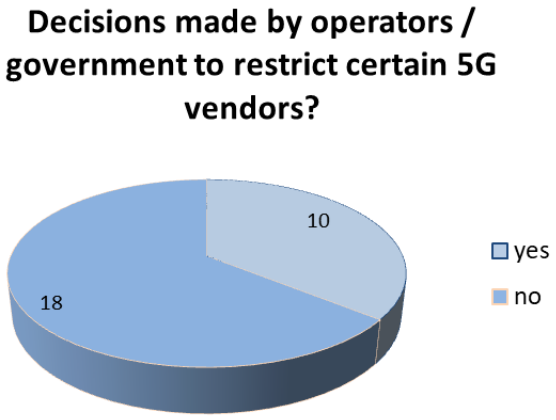
Figure 4-6: Selection criteria for ICT vendors in general regarding digital sovereignty



Source: WIK-Consult, referring to EU27 and the UK.

With regards to 5G vendors, all European countries are required to conduct a national risk assessment, and thus for almost all countries there are indications of ongoing activities reviewing suppliers of 5G components. As of October 2020, in 10 out of the 28 countries, decisions have been taken to restrict certain 5G vendors either by the government or by the operators. However, in 6 more countries, there are proposals for restricting certain 5G vendors; this figure is expected to increase.

Figure 4-7: Selection criteria for 5G vendors regarding digital sovereignty



Source: WIK-Consult, referring to EU27 and the UK.

While security concerns are mostly discussed in the context of 5G, it is clear that the 5G risk assessment review will have an impact for the existing mobile networks as well. Some European countries have already stated that additional security measurements for 5G will also apply to earlier generations of mobile networks.

The European toolbox on 5G Cybersecurity recommends that Member States should strengthen security requirements for mobile network operators. This is done by assessing the risk profile of suppliers, applying restrictions for suppliers considered as high risk, including necessary exclusions for crucial infrastructure, and ensuring that each operator has an appropriate multi-vendor strategy to avoid dependency on a single supplier. From the benchmark, in this respect, we observed different approaches among the Member States; from an explicit prohibition of using "high risk vendors" in the building of "critical" parts of the network (FR, EE, and UK) to an increased set of security requirements including certification, monitoring and notification obligations either upon purchasing or in the event that security issues occur (AT, DE, NL, IR, IT, GR, PT, BE, DK, PL, SI, and SE).[55]

As previously mentioned, the first concrete measurements observed in the benchmark against Chinese 5G suppliers have taken place in the UK during January 2020, where the use of technology supplied by Huawei was initially restricted to 35% in the less sensitive "periphery" of the 5G networks. [56] This regulation could be tightened further as plans were announced in October 2020 to set a phase out date of Huawei by 2027.[57]

Furthermore, in the Netherlands and Italy, Huawei was no longer allowed to provide 5G components for the core networks according to decisions from respectively the incumbent KPN itself [58] and the Italian government, who vetoed a deal between Fastweb and Huawei due to insufficient diversification of vendors.[59]

In Sweden and Belgium, Chinese vendors Huawei and ZTE were not only excluded from providing technology for the core network but also for the Radio Access Network (RAN) based on security issues. In Sweden, the decision was made by the nation regulator, PTS, [60], while in Belgium it was the leading operators Proximus and Orange.[61]

---

55 Just before the work on the present report was completed, the ban of Huawei equipment in Sweden was halted by a court decision. See https://uk.reuters.com/article/us-sweden-huawei-appeal/sweden-halts-5g-auction-after-court-grants-relief-to-huawei-idUKKBN27P2IA Furthermore, a court ruling in France suggests that some French network operators may receive some compensation for removing Huawei equipment from their networks. See https://www.telecompaper.com/news/bouygues-telecom-and-sfr-move-ahead-with-compensation-case-against-govt-in-dispute-over-huawei-equipment--1362354.

56 The Guardian, 22 May 2020, https://www.theguardian.com/technology/2020/may/22/boris-johnson-forced-to-reduce-huaweis-role-in-uks-5g-networks.

57 See https://telecoms.com/506844/uk-mps-recommend-faster-huawei-removal-if-china-doesnt-behave-itself/.

58 Telecoms.com, 15 October 2020, see https://telecoms.com/506944/kpn-taps-ericsson-to-replace-huawei-in-5g-core/.

59 Telecoms.com, 26 October 2020, see https://telecoms.com/507100/italy-reportedly-blocks-huawei-5g-deal-as-bulgaria-joins-us-clean-network-scheme/.

60 Telecoms.com, 20 October 2020, see https://telecoms.com/507001/sweden-bans-huawei-and-zte-from-its-5g-networks/.

61 Telecoms.com,) October 2020. See https://telecoms.com/506852/belgium-says-bye-bye-huawei-hello-nokia/.

In other Member States, like Ireland and Estonia, there have been proposals and public announcements to not include high-risk vendors in their core networks. The reasons most often cited are cybersecurity concerns and the potential for dependency on individual suppliers.

Mobile network operators however face a difficult choice in this context. There is a limited number of suppliers worldwide which deliver large parts of the 5G technology. The market effectively consists of two vendors with their headquarters in the EU – Ericsson (Sweden) and Nokia (Finland) – and two vendors headquartered in China – Huawei and ZTE.[62] Usually, mobile network operators rely on more than one vendor to supply components for their networks in order to ensure resilience. It is also common practice that mobile network operators and vendors develop long-term relationships which may increase the efficiency of collaboration. Furthermore, investment decisions and ordering of 5G components take place well in advance of implementation and activation of the networks and thus have already been decided in several countries (DE for example). To cater for these concerns, it seems that phase out terms are used enabling network operators who have already bought and/or installed components from excluded suppliers to migrate gradually. In the UK, a phase out deadline for Huawei is proposed by 2027, and in Sweden, by 2025 for Huawei and ZTE.

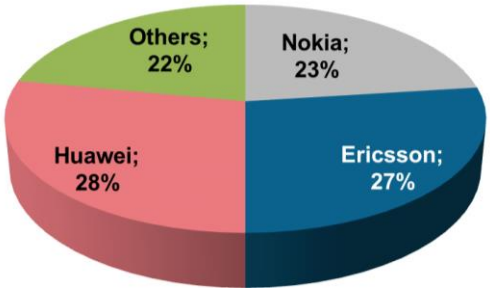
To put this in perspective, Figure 4-8 shows the estimated market shares of suppliers of 4G mobile infrastructure in Europe. As 5G network infrastructure is being rolled out in Europe, there is currently no data available on market shares for 5G infrastructure, but it is clear that Huawei could obtain a significant market share. The existing 4G market share in Europe is a good indication since a mobile operator would usually remain with its current 4G supplier to avoid backward compatibility problems between the two networks.[63] Besides European vendors Ericson and Nokia, Huawei has almost 30% of the market in Europe. Additionally, we reviewed the number of public announced 5G trials per supplier in Europe.[64] Figure 4-9 provides an overview of the vendors involved in 155 unique 5G test trials in Europe. Again, besides Ericsson and Nokia, Huawei takes a similar share in absolute 5G test trial involvements.

62 Dell'Oro Group, see https://techblog.comsoc.org/2020/09/08/delloro-telecom-equipment-revenues-to-grow-5-through-2020-huawei-increases-market-share/.

63 Backward compatibility is that 5G mobile network devices networks can fall back at 4G networks in case 5G networks are not available. This is important when new networks are rolled out and do not yet have comprehensive coverage.

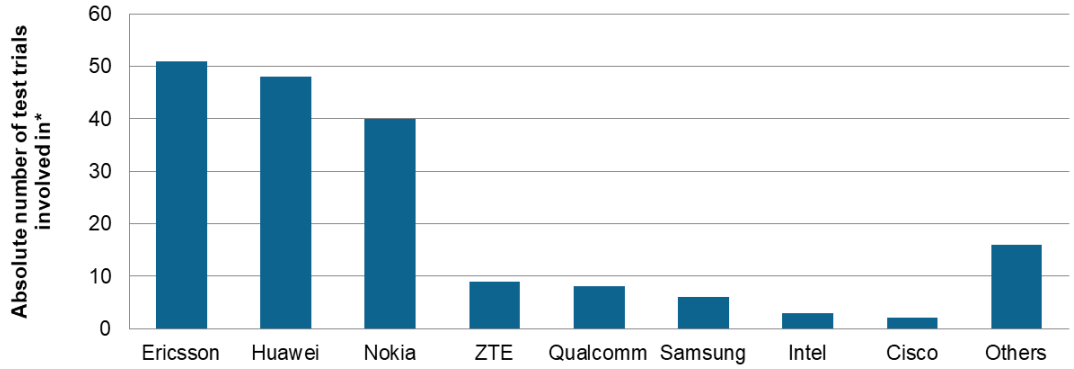
64 Publicly announced 5G trials in Europe to test download speeds, applications (such as virtual and augmented reality, 360° live video and 4K video streams) or interoperability.
Source: www.5Gobservatory.eu.

Figure 4-8: Estimated marketshare of suppliers of 4G mobile infrastructure in Europe



Source: Lightreading.com, 24 February 2020, “Ericsson, Huawei & Nokia's 5G 'wins' are no big deal” by Ian Morris, https://www.lightreading.com/5g/ericsson-huawei-and-nokias-5g-wins-are-no-big-deal/a/d-id/757677.

Figure 4-9: Number of 5G trial per supplier in Europe (until June 2020)



* Note: In some cases, more than one vendor is involved in the same test trial. Hence, the sum of the number of absolute involvements exceeds the number of 155 unique test trials. Source: 5gobservatory.eu.

4.4 Summary table of EU country reports

The following table summarises the approaches taken in each country regarding digital sovereignty. For the more extensive country reports see the Annexes.

Where a country’s approach towards digital sovereignty is labelled as ‘narrow’, this means that it is equated with cybersecurity and that the issue of digital sovereignty is currently not at the forefront of the political agenda. Countries with a medium scope of digital sovereignty have supplemented the cybersecurity dimension with the privacy dimension of digital sovereignty. Countries with a broad scope of digital sovereignty have pursued strategic initiatives to protect national interests including societal and European values.

Table 4-2: Summary of country approach towards digital sovereignty

Country	High level summary of approach towards Digital Sovereignty
Austria	Austria mostly focuses on cybersecurity and data sovereignty for its citizens. Currently, there are also stricter foreign direct investment rules for critical infrastructure planned. The general scope of digital sovereignty can be described as medium.
Belgium	Belgium follows an open government data strategy and pushed an independent data exchange platform for the development of Artificial Intelligence. Its scope of digital sovereignty can be considered as medium.
Bulgaria	Bulgaria does not have digital sovereignty on its agenda as it struggles with digitalisation in general. The national cybersecurity strategy aims to establish a national system for cybersecurity and resilient digital critical infrastructures.
Croatia	Croatia has a very narrow definition of digital sovereignty, it is on the agenda but only regarding cybersecurity concerns. Due to Croatia's Council Presidency (first half of 2020), the focus towards a broader definition of digital sovereignty is emerging. Croatia has close ties to China regarding technological collaborations.
Republic of Cyprus	Cyprus lacks behind with digitalisation in general and does not have digital sovereignty directly on its agenda. Efforts towards digital sovereignty can only be observed through its cybersecurity strategy.
Czech Republic	The Czech Republic stands close to the US regarding its 5G expansion, having given a joint declaration regarding the security concerns and measurements. However, the country does not explicitly exclude single vendors. It took a firm position in May 2020 stating that (state) sovereignty in cyberspace is a rule of international law and an independent right.
Denmark	Denmark has a broad understanding of digital sovereignty and is especially strong in the data protection dimension. Denmark also profits from large investments from US technology firms into local data centres. Regarding 5G, Denmark's incumbent mobile network operator has sidestepped Huawei in favour of Nokia.
Estonia	Estonia has a broad definition of digital sovereignty and is also the first and only country with a so called data embassy where it stores valuable and sensitive data in a foreign state (Luxembourg). It also signed a MoU with the US regarding the expansion of 5G.
Finland	Finland's scope of digital sovereignty can be considered medium. Its main focus is on cybersecurity. However, it also acknowledges the importance of a national cloud provider for its administrative body. In Finland, the right of privacy of any communication is a basic right that is inviolable and there is a strong legal protection over governmental surveillance of digital information.
France	France is one of the biggest actors to push digital sovereignty; it is a declared goal by French policy makers. After Germany, France is the second largest contributor to the GAIA-X project.[65] France plans to apply stricter selection criteria for vendors for core parts in 5G networks and to exclude vendors such as Huawei.
Germany	Germany is the biggest actor on digital sovereignty. Germany is the main contributor to the GAIA-X project. Germany's federal government has obligations to use information technology "Made in Germany" and so called "focus groups" set by the Ministry of Economic Affairs are strong contributors to the political discussion of digital sovereignty. However, Germany is less restrictive in the exclusion of Chinese vendors for the expansion of its 5G networks.
Greece	Greece, mainly due to its low rank in overall digitalisation, has a narrow definition of digital sovereignty and it is practically not on the agenda at all.
Hungary	Hungary's scope of digital sovereignty ranks medium. The protection of Hungary's sovereignty in its cyberspace is a national interest. A free, democratic and secure functioning of the Hungarian cyberspace based on the rule of law is regarded as a fundamental value and interest.

65 Ongoing proposal regarding an European infrastructure which connects existing cloud services into a homogeneous system, which is secure, trustworthy and sovereign, guaranteeing the confident handling of data and applications.

Country	High level summary of approach towards Digital Sovereignty
Ireland	Digital sovereignty is not on the political agenda in Ireland and aspects of it can only be found in the cybersecurity strategy. Regarding the attitude towards US technology companies, Ireland seems to be very careful as many US firms have their European headquarter in Ireland and this weighs heavily on Irelands policy makers.
Italy	Italy does not have digital sovereignty on its agenda. Digital sovereignty aspects are only found in their cybersecurity strategy. Italy has developed a national cloud and databases of national interest.
Latvia	digital sovereignty does not seem to be on the agenda of Latvia. Regarding 5G, Latvia calls for a EU-blacklist of 5G vendors and does not want to single-handedly exclude any vendor.
Lithuania	Lithuania is only concerned with cybersecurity, hence its definition of digital sovereignty is narrow. Lithuania also signed a declaration with the US which aligns their approach for the expansion of 5G networks.
Luxembourg	Luxemburg strives towards a digitalised nation with focus on its important finance sector and datacentres. Digital sovereignty is based on cybersecurity, but the goal is clearly to protect ICT infrastructure in order to ensure the availability of essential services and economic interest. Unique is the concept of data embassy for Estonia. Luxemburg's scope of digital sovereignty is medium.
Malta	Due to the country's size, Malta promotes itself as a "Test Bed" for ICT infrastructure projects. Although, there does not seem to be interest in the expansion of 5G. Security concerns of 5G dominate the public debate.
Netherlands	The Netherlands are an important contributor for certification of and standards for ICT services and products through EU platforms with focus on digital sovereignty. However, digital sovereignty does not seem to be explicitly defined yet, hence the scope of digital sovereignty is only medium.
Poland	Poland incorporates digital sovereignty especially in the field of cybersecurity but also in the field of open data. Together with the US, it also lobbies against using Huawei for the expansion of 5G.
Portugal	Portugal has a strong focus on network integrity and the defence of cyber-attacks. Portugal has set the maximisation of digital resilience as a national task. Its digital sovereignty scope can be described as medium.
Romania	Although Romania is lacking behind digitalisation in general, it has close ties to the US as large US technology firms are investing in local data centres. Romania has also partnered with the US for its cybersecurity strategy and for the roll out approach of 5G.
Slovakia	Slovakia's only concern regarding digital sovereignty is cybersecurity, hence its general scope of digital sovereignty is narrow. The country is working on a government cloud. No restriction for 5G vendors has been made public.
Slovenia	Slovenia does not have digital sovereignty on the agenda and is more focused on digitalisation in general and the development of the ICT sector. Besides, Slovenia puts effort into the development of Artificial intelligence and a government cloud.
Spain	In Spain, attributes of digital sovereignty can only be found in its cybersecurity strategies. digital sovereignty itself is not explicitly defined and in the media, digital sovereignty is only discussed in the context of EU initiatives.
Sweden	Sweden has a strong focus on data sovereignty and open government data. It raised concerns that public/private data is stored on foreign data centres or on local data centres provided by foreign companies.
UK	Concerning digital sovereignty, the UK is mostly concerned with its cybersecurity. Although the UK states explicitly that in cyberspace, sovereignty must be defended, the country is mostly concerned about state funded hacking. The UK has the most restrictive approach for its 5G expansion and excluded Chinese vendors for this task. For data storage, the UK also seems to want to reduce dependency on US firms.

Source: WIK-Consult.

5 Concluding Remarks

The COVID-19 crisis has accelerated an already emerging trend towards gaining "strategic autonomy" with policymakers in Europe. Within the debate on strategic autonomy, "digital sovereignty" plays a role when it comes down to the autonomy of crucial national ICT infrastructure and controlling one's own data.

The analysis conducted as part of the present report found substantial variation in the terminology used as well as the objectives and rationales attributed to digital sovereignty across the 28 reviewed countries (EU Member States and the UK) and at the EU-level. On a general level, it is concerning that European policymakers cannot concur on the definition of a concept which is apparently central to future innovation, growth and security.

However, three common dimensions of digital sovereignty emerged; (1) cybersecurity, (2) privacy and (3) strategic. The reviewed countries are most aligned on cybersecurity aspects. The main differences found refer to the role that strategic considerations play within the respective approach towards digital sovereignty. In particular, large and economically powerful Member States pursue a proactive approach to digital sovereignty that emphasises the strategic dimension with a view to gain (back) leadership and/or self-determination about the regulations and safeguard access to the technology or data. Smaller Member States tend to take a more reactive stance towards the matter.

For all analysed countries, and in particular the UK – due to the Brexit – and the smaller Eastern European Member States due to their economic and defence dependencies, geopolitical rationales appear to play an important role in decisions regarding measures subsumed under the strategic dimension of digital sovereignty.

Beside the much discussed GAIA-X European cloud solution, there are other noticeable examples of how countries have implemented the strategic dimension of digital sovereignty. Among them the concept of a highly secure 'data embassy' as offered by Luxembourg and already used by Estonia as backup for its data centres. It combines synchronisation and scale while ensuring that European and national regulations are applicable to Member States' data. Given the high capital intensity of data storage and cloud services and the current proposals at European level of significant post COVID-19 funding to support economic development in Europe, this could be an opportune moment for such concepts to gain traction.

Notably, the EU as well as most of the countries analysed appear to be keen in underscoring that neither digital sovereignty nor strategic autonomy push for autarky or protectionism. Clearly, digital sovereignty is about striking the balance between achieving its own autonomy while still maintaining a diversified vendor portfolio and international trade relations, which are so important for many economies in the EU.

6 Methodology

The study team conducted desk research on the initiatives and regulation at European level on digital sovereignty and in the 27 European countries together with the UK. The research took place from begin May 2020 to July 2020 and focused on formal documents regarding cyber security and digital strategy and news articles regarding digital sovereignty in crucial ICT areas such as 5G networks, Artificial Intelligence (AI), data storage and cloud services.

As illustrated in Chapter 1, there is no EU-wide understanding or definition of digital sovereignty. And since most EU Member States (MS) have not specifically defined digital sovereignty nor use terminology such as technological sovereignty or digital sovereignty, we searched for strategies, laws and methods applied in each MS which strengthen and encourage the country's autonomy in the digital area.

The findings described in this report are based on publicly available information. Hence, it may be that countries undertake more activities to gain digital sovereignty than found in public sources. Furthermore, the amount of information found and represented in this report does not automatically correspond with the importance of that topic in the context of digital sovereignty.

Whilst covering all 28 countries -the EU and the UK- , we analysed eight countries which carry particular political weight in more detail than the others. Concretely, we focused on Finland, France, Germany, Italy, Poland, Spain, Sweden and the UK (see table below).

Table 6-1: Overview of benchmarked countries

	Country	Country code	Standard report	Extended report
1	Austria	AT	✓	
2	Belgium	BE	✓	
3	Bulgaria	BG	✓	
4	Croatia	HR	✓	
5	Republic of Cyprus	CY	✓	
6	Czech Republic	CZ	✓	
7	Denmark	DK	✓	
8	Estonia	EE	✓	
9	Finland	FI		✓
10	France	FR		✓
11	Germany	DE		✓
12	Greece	GR	✓	
13	Hungary	HU	✓	
14	Ireland	IR	✓	
15	Italy	IT		✓
16	Latvia	LV	✓	
17	Lithuania	LT	✓	

	Country	Country code	Standard report	Extended report
18	Luxembourg	LU	✓	
19	Malta	MT	✓	
20	Netherlands	NL	✓	
21	Poland	PL		✓
22	Portugal	PT	✓	
23	Romania	RO	✓	
24	Slovakia	SK	✓	
25	Slovenia	SI	✓	
26	Spain	ES		✓
27	Sweden	SE		✓
28	UK	UK		✓

Source: WIK-Consult.

7 Annexes – Country Reports

7.1 Digital sovereignty in Austria

Concerning DS, Austria mostly focuses on cyber security and data sovereignty for its citizens. Currently, there are also stricter Foreign Direct Investment (FDI) rules for critical infrastructure planned. The general scope can be described as medium.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

Yes. In May 2020, during a United Nations event, Austria announced its position on whether DS is "*merely a principle, or also a rule of international law*" (the latter). Together with the Czech Republic, both states took this position. Austria referred to the principle of state sovereignty in the context of recent cyber-attacks. "*A violation of this rule constitutes an internationally wrongful act – if attributable to a state – for which a target state may seek reparation under the law of state responsibility. A target state may also react through proportionate countermeasures.*"[66]

In the 2016 Digital Roadmap, the strategy paper for digitalisation published by the Federal Ministry for Digital and Economic Affairs, one of the twelve key principals is to actively shape the European digital single market. The strategy paper does not define digital sovereignty but only data sovereignty of its citizens. Hence, sovereignty is only defined in the context of privacy protection: The data sovereignty of consumers in digital markets must be secured while confidence in digital products and services must be strengthened. The overriding goal is a modern, simple and clear data protection at a high standard, which at the same time preserves the opportunities of digitization and new technologies and includes the digital single market.[67]

In a 2018 letter on "State Sovereignty in the Digital Age" for the Austrian parliament by the Vienna based Institute of Technology Assessment, the research institute further defines sovereignty as self-determination and the ability to make independent and autonomous decisions (e.g. about software solutions and data management). In the letter, it is also stated that "*sovereignty does not necessarily require self-sufficiency but that it is about path dependency in information technology infrastructures, and that dependence on monopolies would endanger this sovereignty".* [68] The institute recommended to first analyse the respective approaches to become aware of the

66 https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/.

67 Federal Ministry for Digital and Economic Affairs (2018): Digital Roadmap Austria, available at: https://www.bmdw.gv.at/Digitalisierung/DigitalisierunginderVerwaltung/Seiten/Digital-Roadmap-Austria.aspx.

68 Institute of Technology Assessment. 2018. Staatliche Souveränität im digitalen Zeitalter. *Foresight und Technikfolgenabschätzung - Monitoring von Zukunftsthemen für das Österreichische Parlament.* https://www.parlament.gv.at/ZUSD/FTA/009_digitale_souveraenitaet.pdf.

issues and thereafter start a comprehensive discussion with regard to a democratically controlled digital sovereignty.[69]

What is the approach towards DS?

Based on the individual MS risk assessments, the NIS Cooperation Group published an "EU toolbox for risk minimisation measures" in January 2020. On the basis of the results of the risk assessment, the Austrian Regulatory Authority for Broadcasting and Telecommunications will draft a proposal for a regulation with the aim to regulate aspects of network information security on the one hand and special topics of 5G security (5G Toolbox of the European Union) on the other hand.[70]

Furthermore, the government is working on new FDI regulations which will make it more difficult to take over Austrian companies in sectors ranging from AI and robotics, to water, infrastructure and food production.[71]

Digital sovereignty and technological aspects

Are there selection criteria for hardware / software vendors?

Network operators are subject to comprehensive requirements by the Telecommunications Act (TKG) and data protection. These obligations must always be met by operators, regardless of all technology and procurement decisions. The Austrian Regulatory Authority for Broadcasting and Telecommunications is responsible for ensuring compliance; it is currently preparing an ordinance under §16a TKG as a contribution to further increasing network security and implementing the European Union's "5G Toolbox". With this, Austria is implementing the European approach of defining security standards with regards to network construction and operation, especially for 5G networks, and making them binding for all suppliers.[72]

In a written parliamentary question on the topic of "Crypto and 5G", the question on how to prevent backdoors in software for cyber espionage by private companies was asked. Chancellor Sebastian Kurz answered "*that this risk may always remain but can be minimised with the framework of a certification or authorization procedure".* [73] Furthermore, Kurz said in a news conference in Vienna in January 2020 that the most important issues regarding the expansion of the 5G network were ensuring security and preventing a unilateral dependence on a supplier. "*We want to be technology-neutral and at the same time guarantee maximum safety*," Kurz said when asked about the government's stance regarding Chinese 5G vendor Huawei, adding: "*We are in close coordination with our European partners and also with the European Commission*"[74].

---

69 Article available at https://www.oeaw.ac.at/ita/detail/news/article/digitale-souveraenitaet-in-oesterreich/.

70 Federal Ministry of Regions, Agriculture and Tourism of the Republic of Austria. 2020. 653/AB Answer on Parliamentary Question 633/J (XXVII. GP).

71 https://www.sn.at/wirtschaft/oesterreich/neuer-anlauf-fuer-schutz-von-firmen-gegen-auslands-uebernahmen-86078275.

72 Federal Ministry of Regions, Agriculture and Tourism of the Republic of Austria. 2020. 960/AB Answer on Parliamentary Question 953/J (XXVII. GP).

73 Federal Chancellery of the Republic of Austria. 2020. 953/AB Answer on Parliamentary Question 955/J (XXVII. GP).

74 Reuters. https://www.reuters.com/article/us-austria-5g-huawei-tech/austria-to-collaborate-with-eu-partners-on-huawei-5g-decision-idUSKBN1ZJ10R.

In another answer to a parliamentary question from 20 March 2020, the responsible Federal Ministry of Regions, Agriculture and Tourism states: "*Telecommunications companies are responsible for the network rollout, which is why they are also responsible for selecting the network vendors. The legal regulations of the Telecommunications Act and the relevant ordinances apply*". Furthermore, "*no assessment is made as to which companies are able to supply components for the rollout of the Austrian 5G networks*"[75].

Are there discussions on other technology aspects with an impact on DS?

In the context of big data and cloud infrastructure, the Data Market Austria research project establishes a data services ecosystem in Austria by creating a technology base for secure data markets and cloud interoperability. The "central node" runs on the Open Telekom Cloud (Deutsche Telekom) and distributes requests to either the same or other Clouds.[76] The three-year project was managed by the Research Studios Austria Forschungsgesellschaft and funded by the Ministry of Transport. Prototype technologies were presented that can handle data trading on a national platform in an automated and secure way and in compliance with all regulations.[77]

Digital sovereignty with regard to skills, norms and educational aspects

Are there specific 'seals' which promote DS?

The "Austrian Cloud" seal of approval enables providers of Austrian cloud solutions to explicitly point out that they offer an Austrian cloud solution. It makes it easier for users to find companies which store their data solely in Austria.[78]

Are there (educational) programs to develop competencies, which can improve DS?

School 4.0 promote digital skills (basic understanding of the flow of digital processes, targeted promotion of IT user competence and responsible use of media) for Austrian school students. Fit4Internet is a platform for increasing digital skills in Austria (understanding the digital basics, the handling of information and data, the ability to communicate and cooperate, the creation of digital content, the safety-conscious behaviour and the ability to solve problems and continue learning).[79]

KMU DIGITAL launched in 2017 and is a research and innovation support initiative targeted at SMEs. The Digital Innovation Hubs focus on social media, mobile services, cloud, IoT, cyber security, robotics and automation machinery, big data and data analytics, 3D-printing and AI. The initiative started in 2018 by the Federal Ministry of Digital and Economic Affairs and is targeted at SMEs.[80]

---

75 Federal Ministry of Regions, Agriculture and Tourism of the Republic of Austria. 2020. 653/AB Answer on Parliamentary Question 633/J (XXVII. GP).
76 Data Market Austria. 2017. D4.1: First Version of the DMA Federated Cloud. https://datamarket.at/wp-content/uploads/2017/01/DMA-Deliverable-4_1-V1.0-Final.pdf.
77 For an English description of the research project, see: https://www.ait.ac.at/en/research-topics/data-science/projects/dma/; project website: https://datamarket.at/en/.
78 https://austriancloud.eurocloud.at/.
79 https://www.fit4internet.at/.
80 https://www.ffg.at/dih.

The Pilot Factories initiative started in 2018 with the focus on smart electronic based systems, discrete manufacturing and process engineering.[81]

81 http://pilotfabrik.tuwien.ac.at/en/.

7.2 Digital sovereignty in Belgium

Belgium follows an open government data strategy and pushed an independent data exchange platform for the development of its AI. Its scope of DS can be considered medium.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

The Belgian Cybercrime Centre of Excellence for Training, Research, and Education (B-ccentre), was the first main coordination and collaboration platform involved in tackling cybercrime in Belgium. The B-CCENTRE project came to an end in November 2014. [82]

In 2015, the Federal Minister of Digital Agenda, Post and Telecommunications launched a federal action plan "Digital Belgium" with the long term digital vision of Belgium. One of the goals was digital confidence and security. The government further established in 2016 the Centre for Cybersecurity in Belgium (CCB), which is also responsible for the national computer emergency response team (CERT). [83]

What is the approach towards DS?

Belgium was the first nation in the EU to transpose the EU NIS Directive.[84] The cybersecurity law imposes obligations on operators of crucial facilities (like digital infrastructures) to take technical and organizational security measures to prevent incidents or to limit their impact and ensure the continuity of services. Operators should set their security objectives, confirm to security standards (like ISO/ICE27001) and implement technical and organisational security. Thereafter they should monitor and notify any breaches to the national Centre for Cyber Security.

Based on the available data, digital sovereignty is 'implemented' in Belgium purely with a focus on developing skillsets with the labour force and companies for economic reasons. No specific measures have been found which focus on decreasing the dependency of certain providers of crucial components for the digital sector.

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors?

No, there are no (published) selection criteria at the moment. Chinese vendors such as Huawei and ZTE are important providers of 5G technology in Belgium. In March 2019, Belgium's centre for cybersecurity found that there was no evidence to indicate that telecom equipment supplied by Huawei Technology could be used for spying. [85]

---

82 https://www.b-ccentre.be/.
83 http://digitalbelgium.be/en/.
84 EU Directive 2016/1148 on security of network and information Systems, 9 May 2018.
85 https://www.brusselstimes.com/belgium/88263/belgian-security-services-want-second-highest-security-level-for-huawei-5g-technology/.

However, in early 2020, the Belgian security services advised Telecom Minister Philippe De Backer to raise the required security level for the 5G networks from 1 to level 4 (EC defines level 1 to 5) that would enable setting restrictions on the use of technology from unreliable vendors.[86] The government of Belgium still needs to decide on the approach to follow in this context.

Belgium is under pressure from the USA in this respect as there are many umbrella organisations active in Brussels, such as NATO. The USA is of the opinion that Chinese law requires Chinese 5G vendors to provide data collected on their networks worldwide to the Chinese government. The Chinese government denies the presence of such an obligation.[87] In October 2020, both Proximus and Orange Belgium announced to replace Huawei's radio access network with Nokia and Ericsson after a "*thorough competitive process, based on technological, operational and financial criteria*."[88]

Are there discussions on other technology aspects with an impact on DS?

Belgium aims to become the AI player in Europe via the 'AI 4 Belgium' coalition. It uses an independent data exchange platform, which enables the re-use of data in a secure manner by third parties with the risk of re-identification of individual data.[89] However, the Belgian government still needs to implement this.

Belgium has a Public Cloud First strategy, which promotes 'G-cloud' services offered by (Belgium) private companies in public cloud environments and services housed in state-owned data centres. These services are managed by the State, allowing for significant cost savings while facilitating roll-out of new applications and technologies.[90] Furthermore, Belgium has a federal open data strategy, which aims to regulate the re-use of government information.

Digital sovereignty with regard to skills, norms and educational aspects

Are there specific 'seals' which promote DS?

Our research did not identify any such measures.

Are there (educational) programs to develop competencies, which can improve DS?

Several initiatives also provide training and certification targeting the youth, unemployed and start-ups, such as DigitalChampions.be, BeCentral[91], the Digital Belgium Skills Fund, the Action Plan ICT and Digitization VDAB, the Digital School, WallCode Digital Wallonia and Fablab Mobile, with a total funding of at least EUR 82.477 million for 2014-2022.[92]

86 De Morgen, 9 January 2020, https://www.demorgen.be/nieuws/veiligheidsdiensten-waarschuwen-regering-voor-5g-van-huawei~b061d88c/?referer=https%3A%2F%2Fwww.google.com%2F.
87 https://www.vrt.be/vrtnws/de/2020/03/07/wer-wird-belgien-mit-5g-ausstatten-duerfen/.
88 Telecoms.com, 9 October 2020, https://telecoms.com/506852/belgium-says-bye-bye-huawei-hello-nokia/.
89 AI4Belgium, report, https://www.ai4belgium.be/wp-content/uploads/2019/04/rapport_nl.pdf.
90 http://digitalbelgium.be/.
91 http://digitalbelgium.be/.
92 EC_DESI 2019, https://ec.europa.eu/information_society/newsroom/image/document/2019-32/country_report_-_belgium.

7.3 Digital sovereignty in Bulgaria

Bulgaria does not have DS on its agenda as it struggles with digitalization in general. The national cyber security strategy aims to establish and develop the national system for cyber security and resilience as well as to support protection and sustainability of digitally dependent critical infrastructures.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

Main focus is on cyber security. No further mentioning of Digital Sovereignty at government level. Bulgaria has a National Cyber Security Strategy and National Network and Information Security Strategy, for which responsibility lies at the Council of Ministers, assisted by the newly established Cyber Security Council and the National Cyber Security Coordinator. Furthermore, there is a "National Security" State Agency[93], mandated to protect strategic communication and information systems from potential cyber security incidents, and to create a Monitoring and Incident Reaction Centre.

What is the approach towards DS?

Bulgaria's national Cyber Security Strategy, named Cyber Resilient Bulgaria 2020 launched in July 2016. The strategy sets out 9 main objectives including its cyber and information security strategy. Within this strategy – among others – the Bulgarian Government is aiming to establish and develop the national system for cyber security and resilience as well as to support protection and sustainability of digitally dependent critical infrastructures. Furthermore, the government is willing to increase its efforts on cyber defence and protection of national security and to raise awareness, knowledge and competencies and develop a stimulating environment for research and innovation in the field of cyber security. [94]

Furthermore, during the NATO Defence Ministers' meeting in October 2016, Bulgaria signed a Memorandum of Understanding with NATO to facilitate information-sharing on cyber threats and best practices, improving the prevention of cyber incidents and increasing Bulgaria's resilience to cyber threats.[95]

How is DS translated into concrete political and regulatory measures?

Bulgaria signed end October 2020 together with North Macedonia and Kosovo the "Clean Network" security agreement. This agreement with the United States regarding high-speed wireless network security aims at excluding Chinese hardware providers.[96]

---

93 https://www.dans.bg/en.
94 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-6.
95 https://www.nato.int/cps/en/natohq/news_137069.htm.
96 https://apnews.com/article/europe-kosovo-china-bulgaria-6d924535309cc2d80574f918087b2ce6.

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors in general?

Our research did not identify any such measures. The two operators planning to offer 5G services (A1 and Telenor) have announced they will be supported by respectively Nokia[97] and Huawei[98].

Is there a discussion on other technology aspects with an impact on DS?

The Bulgarian government is preparing its national AI strategy, while also preparing specific policy reports focusing on education, training, and research.[99]

The European declaration on high-performance computing (HPC) has been signed at 17 October 2017 in Sofia by Bulgarian Minister of Education and Science. Bulgaria was the tenth MS who is joining the European effort to build the next generation of computing and data infrastructures.

> The objective of this declaration is the establishment of a joint cooperation framework between the signatory countries to acquire and deploy an integrated supercomputing infrastructure capable of at least 10^{18} calculations per second […]. The countries have agreed to work together to develop a world-class HPC ecosystem based on European technology and relying on energy-efficient computing via low-power chips.[100]

Digital sovereignty with regard to skills, norms and educational aspects

Are there specific 'seals' which promote DS?

Our research did not identify any such measures.

Are there (educational) programs to develop competencies, which can improve DS?

There are several national programs which contain elements, aiming to develop digital skills in general, but no specific mentioning of aims to increase the digital sovereignty of Bulgaria:

- "Digital Bulgaria 2025": sub goal is to enhance the digital competence and skills in Bulgaria[101]; and
- "Better Science for a Better Bulgaria 2025'' promotes better R&D.[102]

97 https://www.commsupdate.com/articles/2019/07/02/a1-bulgaria-starts-trials-of-5g-technology/.
98 http://yassenguev.com/telecommunication-storm-huawei-5g-shifts-on-the-bulgarian-market/.
99 https://www.oecd.ai/dashboards/countries/Bulgaria.
100 https://ec.europa.eu/digital-single-market/en/news/bulgaria-latest-country-sign-european-declaration-high-performance-computing.
101 https://www.mtitc.government.bg/en/category/85/draft-national-program-digital-bulgaria-2025.
102 https://era.gv.at/object/document/2763/attach/BG_Better_ScienceBetter-final_en.pdf.

7.4 Digital sovereignty in Croatia

Croatia has a very narrow definition of DS. It is on the agenda but only regarding cyber security concerns. Because of Croatia's European Council Presidency (first half of 2020), there was a focus towards a broader definition of DS

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

According to the National Cyber Security Strategy[103], digital sovereignty in Croatia takes the form of the control and prevention of various deviations in the normal functioning of a certain kind of communication and information systems. "*Deviations in the proper operation of these interconnected systems or their parts are no longer merely technical difficulties; they pose a danger with a global security impact."*[104] Croatia aims to prevent and/or control such deviations with relevant cyber security measures focused on the following areas: [105]

- Public electronic communications from planning to building, maintaining and using, electronic communication infrastructure as well as related equipment.
- E-government: establish a system with the necessary level of security of public registries and operate it on the basis of clearly defined rights, obligations and responsibilities of the competent public sector bodies.
- National Critical Infrastructure: the systems, networks and objects of national importance whose disruption in operation or interruption in the delivery of the goods can have serious consequences for national security, health and lives of people, property or environment, security and economic stability and continuous functioning of the government.

Moreover, alongside with cyber security, Croatia seems to put emphasis on data protection as a crucial aspect of digital sovereignty.[106] Among the priorities of Croatia are the following aspects:[107]

- Security of 5G networks;
- Legal and ethical implications of artificial intelligence and defining standards for new technologies;
- Personal data protection and protection of privacy;
- Building professional and technological capacity in the area of cyber security.

103 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/croatian-cyber-security-strategy.
104 https://www.tandfonline.com/doi/full/10.1080/00051144.2017.1407022.
105 https://cip.gmu.edu/2016/08/18/critical-infrastructure-security-resilience-republic-croatia/.
106 https://edps.europa.eu/sites/edp/files/publication/20-01-16_speech_zagreb_en.pdf.
107 https://eu2020.hr/Uploads/EUPDev/files/priorities-of-the-croatian-presidency.pdf.

What is the approach towards DS?

The approach of Croatia is mainly focused on cyber security.

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors in general?

Following the European Commission's recommendations on 5G networks, the Croatian Regulatory Authority for Network Industries (HAKOM) will define criteria for equipment suppliers wishing to operate on the Croatian market and will award frequencies for 5G by the end of 2020.[108]

In regards to security guidelines, the Croatian Law on Electronic Communications sets the rules governing high-speed electronic communications networks. However, there are no rules specified for 5G services.[109]

Noteworthy in this context is a memorandum of understanding signed between Croatia's Central State Office for the Development of Digital Society and Huawei for cooperation in digitization and digital transformation. *"The memorandum provides for continued communication and stronger cooperation between Huawei and Croatia in developing 'smart city' solutions, exchanging expertise, and industrial standards […]."*[110]

Is there a discussion on other technology aspects with an impact on DS?

The Croatian government is currently working on its national strategy for AI.[111]

Regarding cloud services, one of the objectives was to provide *"systematic support in developing user-oriented electronic services of the public administration, to ensure an optimized development of computer infrastructure [...] owned by the Republic of Croatia («public sector cloud» strategy)*" and to *"enable the use of joint interoperable solutions on EU level*"[112]. Croatia has a Government Cloud – Shared Services Centre (CDU), which aims by 2023 to have connected 300 state administration institutions. It will provide digital work stations for 110.000 civil servants.

The Croatian Science and Education Cloud – CRO-SEC:

> The goal of the project is to build a computer and data cloud which will constitute an integral component of national research and innovation e-infrastructure. It was designed as common infrastructure which will enable the services of virtual computer and storage resources on the principle of cloud computing, grid resources, high performance computing resources, large storage capacities and interconnection with European e-infrastructures. […] This implies the development of a computer and data cloud as the key component of the national research and

108 https://www.total-croatia-news.com/business/41219-5g.
109 https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g/croatia.
110 https://vlada.gov.hr/news/croatia-and-china-open-ambitious-chapter-in-economic-and-trade-relations/25727.
111 https://ec.europa.eu/knowledge4policy/ai-watch/croatia-ai-strategy-report_en.
112 Ministry of Public Administration – May 2017: e-CROATIA 2020 STRATEGY, p. 19, https://uprava.gov.hr/UserDocsImages/Istaknute%20teme/e-Hrvatska/e-Croatia%202020%20Strategy%20-final.pdf.

> innovation infrastructure. In addition […] infrastructure for cloud computing, high-performance computing of 25000 processor cores and high-capacity storage of 7 PB will have been established by the end of 2023.[113]

Digital sovereignty with regard to skills, norms and educational aspects

Are there specific 'seals' which promote DS?

Our research did not identify any such measures.

Are there (educational) programs to develop competencies, which can improve DS?

The focus in Croatia is on developing digital skills in general, not specifically on DS.

The Centre for Information Security (CIS) focuses at educating the public on information security via educational materials and events to raise awareness. In addition, a national strategy, Croatia 2030, addresses the development of digital skills through the entire society via several policies and in 2018, the 'Digital Citizen' project was launched with the support of Google. This project was designed to bring digital skills to local communities through public libraries transformed into digital innovation centres.

Croatia has launched a National Digital Skills and Jobs Coalition. The goal is full cooperation with business, educational institutions and the public and private sectors, and to encourage young people to pursue their careers in ICT.[114]

113 Ministry of Public Administration – May2017: e-CROATIA 2020 STRATEGY, p. 66, https://uprava.gov.hr/UserDocsImages/Istaknute%20teme/e-Hrvatska/e-Croatia%202020%20Strategy%20-final.pdf.

114 https://digitalnakoalicija.hup.hr/koalicija.

7.5 Digital sovereignty in Cyprus

Cyprus has a low degree of digitalisation and does not have DS on its agenda. Efforts towards DS can only be observed through its cyber security strategy.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

No specific documents found on DS. Cyprus has a national Cybersecurity Strategy, which aims to mitigate the effects of threats in cyberspace and the protection of critical infrastructures (beyond ICT). [115]

The Cypriot Government focuses on digitalization but not digital sovereignty specifically. For example the Cyprus Productivity Centre launched an educational program to minimize digital illiteracy and further promote the use of eGovernment services. Also, the Justice system initiated a key reform to adopt a web-based Court administration system (e-Justice system).[116]

What is the approach towards DS?

No specific approach towards DS. Merely a digitalisation strategy for the period 2012-2020 aiming to develop the information society in Cyprus.[117] It includes for example infrastructure roll-out, eGovernment, eHealth, eLearning and green ICT.[118]

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors in general?

Our research did not identify any such measures.

Is there a discussion on other technology aspects with an impact on DS?

In January 2020, the Council of Ministers has approved the National Artificial Intelligence strategy of Cyprus. Beside the economic implication of the new technology, Cyprus will also focus on creating national data areas and developing ethical and reliable AI.[119] No rules to support EU/nationwide cloud have been tracked, probably due to Cyprus' low level of technological and digital innovation.

115 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-cyprus.
116 https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Cyprus_2019_0.pdf.
117 https://ec.europa.eu/digital-single-market/en/news/digital-strategy-cyprus.
118 https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Cyprus_2019_0.pdf.
119 https://ec.europa.eu/knowledge4policy/ai-watch/cyprus-ai-strategy-report_en.

Digital sovereignty with regard to skills, norms and educational aspects

Are there specific 'seals' which promote DS?

Our research did not identify any such measures.

Are there (educational) programs to develop competencies, which can improve DS?

No specific programs on improving DS, merely general digitalisation like how to use ICT at schools[120] and how to use the internet safely and ethical aspects (Safer Internet Program by Connecting Europe Facility (CEF) and Cyber Ethics funded by the European Commission's Innovation and Networks Executive Agency (INEA)).[121]

120 https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj85b_7qNzpAhWE16QKHX1kB_0QFjADegQIAhAB&url=http%3A%2F%2Fec.europa.eu%2FDocsRoom%2Fdocuments%2F4565%2Fattachments%2F1%2Ftranslations%2Fen%2Frenditions%2Fpdf&usg=AOvVaw1WPThYftUDEuQdR6571l2l.

121 https://www.newstrategycenter.ro/wp-content/uploads/2019/07/George_Michaelides_Cyber_Security_Strategy_of_RoCyprus.pdf.

7.6 Digital sovereignty in the Czech Republic

The Czech Republic signed a joint declaration with the US regarding the security concerns and measurements for 5G. However, the country does not explicitly exclude single vendors. The Czech Republic took in May 2020 a firm position that (state) sovereignty in cyberspace is a rule of international law and an independent right.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

On 11 May 2020, the Czech Republic took a firm position during a United Nations event that digital sovereignty is a rule of international law, by recognizing the existence of an independent obligation to respect sovereignty in cyberspace. They consider "*the principle of sovereignty as an independent right and the respect to sovereignty as an independent obligation*. *The Czech Republic firmly believes that […] both aspects of sovereignty in cyberspace, be it an internal one, with the exclusive jurisdiction over the ICTs […] located on its territory, or the external one, including the determination of its foreign policy, subject only to obligations under international law*."[122]

There are several government driven programs aiming to stimulate the digitalisation, like Digital Czechia, Czech Republic in Digital Europe, the Information Strategy of the Czech Republic and Digital Economy and Society. However, there is reference to digital sovereignty (Digital Czechia) and the promotion of priorities, interests and national specifics of the Czech Republic is named (Czech Republic in Digital Europe).[123]

What is the approach towards DS?

Apart from further digitalisation, the Czech Republic also focuses on an EU wide approach of issues like online platform taxation[124] and regulation not only from the consumer protection side but also from the perspective how to stimulate the further growth of these platforms (for example Uber and Airbnb).[125]

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors in general?

Taking into account that secure 5G networks "*will be vital to both future prosperity and national security, the United States and the Czech Republic declared their desire to strengthen their cooperation on 5G*." The parties emphasized "*the importance of encouraging the participation of reliable and trustworthy network hardware and software suppliers in 5G markets, taking into account risk profile assessments, and promoting*

122 https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/.
123 https://www.mpo.cz/en/business/digital-society/digital-czech-republic--243601/.
124 https://www.osw.waw.pl/en/publikacje/analyses/2020-01-29/plans-to-introduce-a-digital-tax-czech-republic.
125 http://www.digital-czech-republic.eu/wp-content/uploads/2018/02/2018_DIGITAL_ENG_WEB.pdf.

frameworks that effectively protect 5G networks from unauthorized access and interference." Parties further recognized that "*5G suppliers should provide products and services that enable innovation and promote efficiency".* They also note that "*all countries share a responsibility to undertake a careful and balanced approach to network security, and the evaluation of 5G component and software providers."* **126**

Is there a discussion on other technology aspects with an impact on DS?

> The Czech Republic and the European Union are fully aware of the fundamental importance of artificial intelligence (AI) and its use for the future development and competitiveness of national, European and global economies and societies. The National Artificial Intelligence Strategy of the Czech Republic […] is therefore primarily aimed at building on the activities and strategic documents of the EU and achieving the full potential of digital transformation. To do so, it sets out a framework of priority objectives and tools to support AI development in the academic, public and private sectors, mutual cooperation and international engagement, which the Czech Republic has committed itself to in the Declaration of Cooperation on Artificial Intelligence signed on 10th April 2018. The National AI Strategy follows up on and meets the objectives of the Government Innovation Strategy 2019–2030 and is linked to the Digital Czech Republic program. It was inspired by similar foreign strategic documents concerning the AI and support for the digitization of the industry and services.**127**

Digital sovereignty with regard to skills, norms and educational aspects

Are there specific 'seals' which promote DS?

Our research did not identify any such measures.

Are there (educational) programs to develop competencies, which can improve DS?

Czech Republic knows several programs aimed at improving the digital skills of its citizens, like the Digital literacy strategy 2015-20**128** and the National Digital Skills program of 2016**129** but there is no specific mentioning of aiming at digital sovereignty.

126 https://www.state.gov/joint-statement-on-united-states-czech-republic-joint-declaration-on-5g-security/.
127 https://ec.europa.eu/knowledge4policy/publication/national-artificial-intelligence-strategy-czech-republic_en.
128 http://pen.ius.edu.ba/index.php/pen/article/viewFile/522/331.
129 http://www.refernet.cz/sites/default/files/cz_2017_news_3_digital_education-2.pdf.

7.7 Digital sovereignty in Denmark

Denmark has a broad understanding of DS and is especially strong in the data protection dimension. Denmark profits from large investments from US technology firms into local data centres. Regarding 5G, Denmark's incumbent MNO has sidestepped Huawei in favour of Nokia.

Digital sovereignty in general

How is Digital Sovereignty defined in the respective country?

In the case of Denmark, according to the country's Cyber and Information Security Strategy 2018-2021, digital sovereignty is perceived as a significant aspect / parameter that will ensure the country's successful and continuous digital transformation. Within this framework, Denmark seems to put emphasis on cyber and information security.[130]

Is digital sovereignty (DS) on the agenda of the government?

Digital sovereignty was initially incorporated in Denmark's first national cyber and information security strategy for 2015-2016, which aimed to enhance the Danish government's cyber and information security efforts as well as to raise awareness of cyber and information security among citizens and businesses. The strategy contained several initiatives aimed at raising awareness of cyber and information security among citizens, businesses and authorities.[131]

Moreover, in the spring of 2018, all parties of the Danish Parliament entered into a new telecommunications policy agreement. One of the main elements of the agreement is the ambition that Denmark must be at the forefront in rolling out 5G, and that Denmark must have the best policy framework for using the newest technology.

In February 2020, Denmark along with Austria, Bulgaria and Romania joined the Euro QCI [132] initiative agreeing to work together with 20 other EU MS towards the development of a quantum communication infrastructure across Europe. The purpose of the QCI will be to boost European capabilities in quantum technologies, cybersecurity and industrial competitiveness.[133]

What is the approach towards DS?

Focus is mainly on cybersecurity and how citizens, businesses and authorities can be assisted to become technologically prepared against threats.[134]

---

130 https://en.digst.dk/policy-and-strategy/danish-cyber-and-information-security-strategy/about-the-danish-cyber-and-information-security-strategy/.
131 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Denmark_2015_DK_NCSS.pdf.
132 Quantum Communication infrastructure.
133 https://ec.europa.eu/digital-single-market/en/news/austria-bulgaria-denmark-and-romania-join-initiative-explore-quantum-communication-europe.
134 https://en.digst.dk/policy-and-strategy/danish-cyber-and-information-security-strategy/about-the-danish-cyber-and-information-security-strategy/.

As part of a political agreement, the government has allocated almost DKK 1 billion until 2025 for the implementation of the initiatives making up the Digital Strategy for Denmark's Digital Growth.[135]

In November 2018, the Danish government decided to prepare a strategy for use of data in the public sector. The strategy aims at creating more coherent and targeted services through data, as well as ensuring a clear framework for use of data.

How is DS translated into concrete political and regulatory measures?

The main regulatory measure is the Act on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the Data Protection Act[136]), published by the Danish Ministry of Justice in May 2018. The Danish Data Protection Agency is the independent authority that supervises compliance with the rules on the protection of personal data.[137]

> In mid-2017, Denmark became the first country in the world to elevate technology and digitalization to a cross-cutting foreign and security policy priority. The initiative was named technological diplomacy, or simply TechPlomacy. […]
>
> Denmark's TechPlomacy initiative aims at addressing three interlinked trends in foreign policy:
>
> First, some of today's most far-reaching societal changes are driven in part or full by technological disruption in different forms and shapes: The impact of artificial intelligence and automation on the future of jobs; big data on the protection of personal information; social media on democratic dialogue and elections; Internet of Things on cyber security; digital business models on taxation systems; and crypto-currency on global financial architecture. […]
>
> Second, the multi-national tech companies driving this technological innovation have become extremely influential; to the extent that their economic and political power match - or even surpass - that of our traditional partners, the nation states. At the same time, it is becoming increasingly difficult for policy-makers at all levels to keep up with the pace and impact of new technologies.
>
> Third, the transformative nature of emerging technologies combined with the rise of powerful non-state actors are shaping foreign policy and geopolitics in new ways. […]
>
> The Danish TechPlomacy initiative is spearheaded by Denmark's (and the world's) first Tech Ambassador. The Office of the Danish Tech Ambassador has a global mandate and a physical presence across three time zones in Silicon Valley, Copenhagen and Beijing - transcending borders and regions and rethinking diplomacy.[138]

TechPlomacy incorporates the following two main operational aspects: (i) The Office of Denmark's Tech Ambassador is responsible to transfer any concerns or questions on behalf of Danish authorities to the tech companies with the aim to influence the direction of technology in favour of Denmark's interests. (ii) Influence the international agenda

135 https://eng.em.dk/media/10566/digital-growth-strategy-report_uk_web-2.pdf.
136 https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf.
137 https://www.datatilsynet.dk/english/.
138 https://techamb.um.dk/en/techplomacy/abouttechplomacy/.

around tech policy in accordance with Danish interests and values, establishing new alliances, multilateral fora, and multi-stakeholder partnerships.

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors in general?

There are no specific selection criteria for hardware / software vendors, but it is clear that relevant regulations are on the way. According to the Danish Cyber and Information Security Strategy 2018-2021, regulatory measures will be activated for suppliers of digital equipment and software operating within the crucial sectors. Government institutions must set clear requirements regarding cyber and information security for providers of IT services and infrastructure, perform regular risk assessments and follow up regularly on providers' ICT security measures.[139]

Is there a discussion on other technology aspects with an impact on DS?

Denmark aims to become a "*front-runner in responsible development and use of artificial intelligence*" – benefitting individuals, businesses and society as a whole.[140] To this aim, there is a Danish National Strategy for Artificial Intelligence, published in March 2019.[141]

DKK 60 million are allocated for new initiatives in the strategy. Among other things, a number of signature projects will be carried out in cooperation with municipalities, regions and private companies.

During the last couple of years, several of the world's largest tech companies pinpointed Denmark as a top European location for data centres:

> Apple is currently building one of the world's largest data centres (potentially 160,000m^2) near the city of Viborg and has acquired a second even larger site near the city of Aabenraa, close to the Danish-German border. Facebook has a 53,000m^2 data centre under construction in Odense, right in the middle of Denmark, and have recently confirmed they are considering a second site near Esbjerg. Last, but not least, Google has acquired two large-scale sites near the cities of Fredericia and Aabenraa respectively for future data centre projects.[142]

The sea cable capacity to other EU MS is increased with three new subsea fibre projects, reducing the dependency of Denmark:

> The Irish fibre cable capacity provider, AquaComms, has announced two subsea cable projects, which are going to land in the Esbjerg/Varde region on the Danish west coast. Furthermore, construction of a combined power and fibre cable, connecting Esbjerg with Emshaven in the Netherlands is underway. This cable is owned by the Danish and Dutch TSO's. The two AquaComms projects are the "Havfrue" cable connecting Denmark with New Jersey in the US, and "North Sea Connect", which will connect Denmark with the UK and Ireland. [143]

139 https://en.digst.dk/policy-and-strategy/danish-cyber-and-information-security-strategy/about-the-danish-cyber-and-information-security-strategy/.
140 https://en.digst.dk/policy-and-strategy/denmark-s-national-strategy-for-artificial-intelligence/.
141 https://eng.em.dk/media/13081/305755-gb-version_4k.pdf.
142 https://data-economy.com/denmark-the-new-digital-hub-in-northern-europe/.
143 https://data-economy.com/denmark-the-new-digital-hub-in-northern-europe/.

Are there discussions specifically on 5G vendors? Specific security guidelines?

The Danish Energy Agency has published the 5G Action Plan for Denmark[144] with the aim to develop and suggest concrete actions in order to make Denmark a front-runner in the use and infrastructure of 5G.

Within February 2019,

> Danish mobile operators Telenor and Telia have enlisted Finnish vendor Nokia to help them test 5G mobile technology from the second quarter of 2019. The tests will utilise the network belonging to TT-Netvaerket, the joint infrastructure company established by the two telecom operators in February 2012.[145]

In March 2019,

> Danish telecom provider TDC has sidestepped China-based vendor Huawei in favor of Sweden-based Ericsson to build the company's 5G network. TDC has had a long-standing relationship with Huawei, which has increasingly come under a microscope due to security concerns.[146]

Are there discussions on other technology aspects with an impact on DS?

DeiC: The Danish e-infrastructure Cooperation (DeiC) coordinates Danish digital infrastructure as an umbrella for the eight Danish universities to ensure delivery of computing, storage and network infrastructure to Danish research, teaching and innovation. DeiC coordinates Danish participation in Nordic and European e-infrastructure organizations and projects.[147]

CLOUD.DK: Cloud.dk is the first Danish public cloud. Cloud.dk focuses on delivery cloud-solutions adapted to the Scandinavian market. The vision is to be the leading cloud-provider in Scandinavia and to offer the most solid, stable and professional alternative to traditional computing and hosting to Danish and Nordic companies. Cloud.dk's data centres are all located in Denmark.[148]

Digital sovereignty with regard to skills, norms and educational aspects

Are there state 'seals of approval' showing a certain compliance and/or quality?

With the support of the Danish government and funding from the Danish Industry Foundation, Danish companies are establishing a seal for "good IT security and responsible data use" with the aim to give Danish companies a boost in data security and make it more attractive for them to handle data responsibly. One of the 8 criteria that a company should meet is "Control of own data".[149]

144 https://ens.dk/sites/ens.dk/files/Tele/5g_action_plan_for_denmark.pdf.
145 https://www.commsupdate.com/articles/2019/02/26/telenor-and-telia-tap-nokia-to-test-5g-in-denmark/.
146 https://www.sdxcentral.com/articles/news/ericsson-ousts-huawei-as-tdcs-5g-vendor-in-denmark/2019/03/.
147 https://www.deic.dk/.
148 https://cloud.dk/en.
149 https://dataethics.eu/danish-companies-behind-seal-for-digital-responsibility/.

Are there (educational) programs to develop competencies which can improve DS?

The Danish Digital Innovation Hubs (DIH) offers currently seven fully operational digital innovation hubs in Denmark.[150]

'SMEs: Digital', one of the initiatives included in the growth plan, helps SMEs exploiting the new digital technologies to create growth and jobs in Denmark. Through www.smvdigital.dk, SMEs can get private procurement grants to help them clarify how they can digitize further and to identify economic and business potential.[151]

150 https://s3platform.jrc.ec.europa.eu/digital-innovation-hubs-tool?p_p_id=digitalinnovationhub_WAR_digitalinnovationhubportlet&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&formDate=1589725153839&freeSearch=&countries=4&evolStages=3&servicesProvided=2&servicesProvided=10&servicesProvided=13&h2020=false.

151 http://www.smvdigital.dk/.

7.8 Digital sovereignty in Estonia

Estonia has a broad definition of DS and is also the first and only country with a so called data embassy where it stores valuable and sensitive data in a foreign state. It also signed a MoU with the US regarding the expansion of 5G.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

Digital sovereignty in Estonia can be defined using a quote from the country's Cybersecurity Strategy for 2019-2022 published by the Ministry of Economic Affairs and Communications:[152]

> Our experience has brought an understanding that in a successful digital society, developing information society and ensuring cybersecurity must be a strategic whole. The role of cybersecurity in the information society is to ensure conditions for efficient and secure use of opportunities offered by ICTs.

A first approach from Estonian government towards digital sovereignty is demonstrated through the 2008 Cyber Security Strategy:

> Estonia's first national strategy document that recognized the interdisciplinary nature of cybersecurity and the need for coordinated action in the area. It was also one of the first horizontal cybersecurity strategies in the world – it was only after the 2007 cyberattacks against Estonia that cybersecurity began to be perceived as an essential part of national security. The Estonian 2008 cybersecurity strategy was among the first of its kind globally.[153]

Following the publication of the 2008 Cybersecurity Strategy, in 2009 the Cyber Security Council was established at the Security Committee of the Government of the Republic. The task of the Council is to contribute to smooth co-operation between various institutions and conduct surveillance over the implementation of the goals of the Cyber Security Strategy. The Council is chaired by the Secretary General of the Ministry of Economic Affairs and Communications.

What is the approach towards DS?

Estonia's Cybersecurity Strategy 2019–2022 lays down four important objectives:[154]

- Estonia is a sustainable digital society relying on strong technological resilience and emergency preparedness.
- Estonian cybersecurity industry is strong, innovative, research-oriented and globally competitive, covering all key competences for Estonia.
- Estonia is a credible and capable partner in the international arena.
- Estonia is a cyber-literate society and ensures sufficient and forward-looking talent supply.

152 https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.
153 https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf.
154 https://www.mkm.ee/en/objectives-activities/cyber-security.

How is DS translated into practical measures?

Following the publication of the 2008 Cyber Security Strategy, Estonia proceeded with relevant regulatory measures publishing the Cybersecurity Act[155] in May 2018. Other relevant legislation are the Electronic Communications Act [156] and the Electronic Identification and Trust Services for Electronic Transactions Act[157].

> Through its e-Estonia initiative, Estonia has built a digital society and developed the most technologically advanced government in the world. Practically every government service is paperless and performed electronically. As a result, Estonia is highly dependent on its information systems and the data stored on them. To protect its data, Estonia developed the concept of data embassies – servers outside the country that are legally under Estonian jurisdiction.[158]
>
> Data Embassy is an extension in the cloud of the Estonian government, which means the state owns server resources outside its territorial boundaries. This is an innovative concept for handling state information, since states usually store their information within their physical boundaries. Data Embassy resources are under Estonian state control, secured against cyberattacks or crisis situations with KSI blockchain technology, and are capable not only providing data backups, but also operating the most critical services. [159]

Data Embassy is actually a data center located in Luxembourg under a Tier 4 level of security – the highest level for data facilities.

> It is fully under the control of Estonia, but has the same rights as physical embassies such as immunity. […] Data Embassy kick-off took place in 2015 and the finalised agreement between Estonia and Luxembourg was signed in 2017. The development of the Estonian Government Cloud is a collaboration between the Estonian Government and private sector companies, including Cybernetica, Dell EMC, Ericsson, OpenNode and Telia.[160]
>
> The purpose of the critical information infrastructure protection (CIIP) is to maintain a trouble-free functioning of the country's essential information and communication systems. The Information System Authority (RIA) organises protection on a national level for the public and private sector network and information systems that are essential for the functioning of the Estonian state.[161]

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware vendors in general?

Estonia effectively ruled out Chinese companies as suppliers of software or hardware for its 5G networks. The governments of Estonia and the US have signed a memorandum of understanding (MoU) which will restrict the use of Huawei equipment in Estonia's 5G mobile core networks[162].

---

155 https://www.riigiteataja.ee/en/eli/523052018003/consolide.
156 https://www.riigiteataja.ee/en/eli/ee/530052018001/consolide/current.
157 https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/527102016001/consolide.
158 https://www.oecd.org/gov/innovative-government/Estonia-case-study-UAE-report-2018.pdf.
159 https://e-estonia.com/solutions/e-governance/data-embassy/.
160 https://e-estonia.com/solutions/e-governance/data-embassy/.
161 https://www.ria.ee/en/cyber-security/critical-information-infrastructure-protection-ciip.html.
162 https://www.aspenreview.com/article/2020/5g-estonia-picks-national-security-technology/.

Estonian officials say that the considerations listed in the MoU do not specifically target Huawei, but affect all manufacturers of 5G technologies. Nevertheless, the thrust of the message is clear. "*We'll assess on a case-by-case basis whether a technology constitutes a security risk for Estonia, or not*," says National Cyber Security Policy Director Raul Rikk. Already in the spring of 2019, the Estonian Foreign Intelligence Service reportedly concluded that Huawei does not meet this criterion.

The details, however, of how the terms of the MoU signed with the United States are to be implemented remain unclear. Estonian officials state that security regulations are not generation-specific, with the same rules applying to 3G, 4G and 5G networks.[163] "*According to the vision established by the Ministry of Economic Affairs and Communications, Estonia's goal is to develop 5G connectivity in a way that would allow the free flow of data, the development of innovative services and the introduction of artificial intelligence".*[164] "*In addition, the Riigikogu's national defence committee decided to initiate a legislative amendment that would allow the government to establish by regulation a requirement for coordination of hardware and software used in communications networks, and the procedures for such coordination. As data flows through communications networks, the committee considers that communications networks are playing an increasingly important role in the context of national security and defence".*[165]

Is there a discussion on other technology aspects with an impact on DS?

Estonia's AI strategy was adopted at Cabinet meeting on 25 July 2019. It is a sum of actions that Estonian government will take to advance the take-up of AI in both private and public sector, to increase the relevant skills and research and development (R&D) base as well as to develop the legal environment. Estonian government will invest at least 10M euros in 2019-2021.

> Estonia is a globally unique state in that nearly all of its core government functions and public services are not only digitized but premised upon the openness and free-flow of data; in essence, it operates 'government as a data model'. At the basis of this model is a secure and interoperable data sharing network called the X-Road which enables citizens, public and private entities to access and manage their own data, as well as records of who has viewed their data. The X-Road operates as a decentralized system, in that there is no one server, data controller, or place where all of an individual's information is held, nor is data duplicated across sources, it is rather shared among those connected.[166]
>
> The implementation of the Government Cloud solution provides an excellent foundation for public e-services and solutions, which makes Estonia the most digital country in the world. […] The Estonian Government Cloud will lead to the modernization and renewal of existing information systems, to embrace the opportunities offered by cloud technology and allow more agility in provision of e-services by the Estonian government agencies and critical service providers to residents and e-residents. […] The Estonian Government Cloud is developed in collaboration between the Estonian Government, represented by the State

163 https://www.aspen.review/article/2020/5g-estonia-picks-national-security-technology/.
164 https://news.postimees.ee/6883472/estonia-planning-to-achieve-5g-connection-in-larger-cities-by-2023.
165 https://www.baltictimes.com/estonia_planning_to_achieve_5g_connection_in_larger_cities_by_2023/.
166 https://medium.com/@sarahlmingle/bordering-states-data-localization-and-its-relationship-to-cyber-sovereignty-in-russia-and-estonia-18c9c31e7db5.

> Infocommunication Foundation (RIKS), and a consortium of private sector companies including Cybernetica, Dell EMC, Ericsson, OpenNode and Telia. [167]

Digital sovereignty with regard to skills, norms and educational aspects

Are there norms or state 'seals of approval' showing a certain compliance and/or quality?

Three-level IT Baseline Security System ISKE[168]

An information security standard is developed for the Estonian public sector.

> According to Government Regulation no. 273 of 12 August 2004, ISKE is compulsory for state and local government organizations who handle databases/registers. The first version of the ISKE implementation manual was completed by October 2003.
>
> The goal of implementing ISKE is to ensure a security level sufficient for the data processed in IT systems. The necessary security level is achieved by implementing the standard organizational, infrastructural/physical and technical security measures.

Are there (educational) programs to develop competencies which can improve DS?

In the cyber security domain, the e-Governance Academy (eGA) focuses on organizational, regulative and technical measures for national cyber security and includes best practice from around the world. eGA assists nations and specific sectors in improving cyber security knowledge, developing policies and legislation, raising organizational and personnel capacity, implementing security technologies, and developing cooperation frameworks.[169]

167 https://e-estonia.com/solutions/e-governance/government-cloud.
168 https://www.ria.ee/en/cyber-security/it-baseline-security-system-iske.html.
169 http://www.ega.ee/.

7.9 Digital sovereignty in Finland

Finland's scope of DS can be considered medium, its main focus is on cybersecurity. However, Finland also acknowledges the importance of a national cloud provider for its administrative body. In Finland, the right of privacy of any communication is a basic right that is inviolable and there is a strong legal protection over governmental surveillance of digital information.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

Digital Sovereignty incorporates the following three key-terms in Finland:[170]

- Cyber security: it encompasses the measures on the functions vital to society and the critical infrastructure which aim to achieve the capability of predictive management and, if necessary, tolerance of cyber threats and their effects, which can cause significant harm or danger to Finland or its population.
- Protection of privacy: the protection against the unlawful or hurtful invasion of personal privacy. Protection of privacy includes the right to privacy and other associated rights in the processing of personal data.
- Information (data) security: Information security means the administrative and technical measures taken to ensure the availability, integrity and confidentiality of data.

The Finnish Government published the first national Cyber Security Strategy in January 2013. The strategy was drafted by the Defence and Security Committee, currently the Security Committee of Finland that is a permanent co-operation body for proactive preparedness. [171]

The national implementation programme of the Cyber Security Strategy was published on 11 March 2014.

What is the approach towards DS?

The following strategic guidelines from the Cyber Security Strategy target (broadly) digital sovereignty:[172]

- Improve comprehensive cyber security situation awareness among the key actors that participate in securing vital functions of society.
- Maintain and improve the abilities of businesses and organisations to detect and repel cyber threats and disturbances that threaten vital functions.
- The Finnish Defence Forces will create a comprehensive cyber defence capability for their statutory tasks.

170 https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.
171 https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.
172 https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.

- Strengthen national cyber security through the active and efficient participation of international organisations and collaborative forums deemed critical to cyber security.
- Improve the cyber expertise and awareness of all societal actors.
- Assign cyber security related tasks, service models and common cyber security management standards to the authorities and actors in the business community.

How is DS translated into practical measures?

In May 2014, the Finnish Minister of Education, Science and Communication Krista Kiuru called for a new fibre-optic cable between Finland and Germany, circumventing Sweden as technical proposal towards achieving digital sovereignty. The Minister quoted:[173]

> Our geopolitical location is based both on geography and on decisions that we make ourselves. We ourselves must first have the courage to develop Finland into a significant safe harbour of information, where companies and countries can safely place their critical data. […] With these kinds of actions we significantly strengthen the image of our country as a concentration of data traffic.

Finland has not only implemented the national provisions required by the GDPR, but also passed a supplementary implementation act of the GDPR, the Data Protection Act of Finland (Tietosuojalaki)[174] on January 1, 2019.

In addition, other key Finnish laws concerning data sovereignty were also implemented:

- The Act on Electronic Communication Services 917/2014 (Laki sähköisen viestinnän palveluista)[175] of January 1, 2015 aims to, inter alia, ensure the confidentiality of electronic communication and the protection of privacy;
- The Act on the Protection of Privacy in Working Life 759/2004 ('Working Life Act') (Laki yksityisyyden suojasta työelämässä) [176] aims to promote the protection of privacy and other rights safeguarding the privacy in working life; and the
- Act on the Processing of Personal Data in Criminal Cases and in connection with Maintaining National Security entered into force on January 1, 2019 along with the Data Protection Act[177].
- In addition, criminal sanctions can ensue from breaches of data protection laws in Finland as the Criminal Code of Finland 39/1889 (Rikoslaki) includes several data processing, data privacy, confidentiality and data security related offences or crimes. Finland has also introduced a new punishable offence, the data protection offence, to the Criminal Code of Finland based on the GDPR. If the controller or data processor commits a data protection offence, the punishment is a fine or up to one year of imprisonment.

173 https://www.lvm.fi/en/-/minister-kiuru-on-submarine-cable-decision-finland-to-be-a-safe-harbour-for-data-795409.
174 https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf.
175 https://www.finlex.fi/fi/laki/ajantasa/2014/20140917.
176 https://www.finlex.fi/fi/laki/ajantasa/2004/20040759.
177 https://www.dlapiperdataprotection.com/index.html?t=law&c=FI.

Based on these laws, Finland has an exceptionally high level of data protection for the individual but also at the collective level.

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors in general?

The Finnish Ministry of Transport and Communications, through the National Cyber Security Centre of Finland, is responsible for applying security measures for 5G networks. The Finnish policy is in line with the EU's Toolbox for 5G Security[178]. The Finnish Transport and Communications Agency (Traficom) supports network operators and equipment manufacturers in using the Toolbox and potential needs for legislative changes will be identified and amendments implemented as part of law drafting work.

Is there a discussion on other technology aspects with an impact on DS?

The Artificial Intelligence Programme was launched with the aim of steering Finland towards the age of AI, taking into consideration measures reaching far into the future and at the same time measures that are relevant today. The work was launched on 18 May 2017, commissioned by Minister of Economic Affairs Mika Lintilä. In the Programme's Final Report, published in June 2019, the following points are mentioned regarding the linkage between artificial intelligence and digital sovereignty: [179]

> AI and the expanding digitalization are rendering the field of security increasingly demanding. […] The National Emergency Supply Agency has launched the Kyber2020 programme to enhance the Finnish security of supply.
>
> The societal importance of digital security is becoming emphasized, which opens up opportunities for companies investing in it and providing relevant services. In collaboration with four partners, the Ministry of Economic Affairs and Employment launched a project, which resulted in the publication of the Growth from digital security roadmap aimed at the development of competence and business related to digital security.

Suomen Huoltovarmuusdata (SHVD) is a data centre established by the National Emergency Supply Agency and its aim is to be top secure service operator for the most critical information technology in Finland. Reason for establishing SVHD came from the Governments decision on the security of supply goals from year 2008, which states that the functions of society's most critical information technology needs to be secured during emergency conditions. In year 2008 established data centre is service provider for the most critical information systems and aims to ensure that the functions of information systems will operate in all conditions.[180]

178 https://valtioneuvosto.fi/en/artikkeli/-/asset_publisher/euroopan-yhteiset-linjaukset-lisaavat-5g-verkkojen-turvallisuutta.
179 http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161688/41_19_Leading%20the%20way%20into%20the%20age%20of%20artificial%20intelligence.pdf.
180 https://www.suomenhuoltovarmuusdata.fi/.

Finland was already well connected via submarine cables[181], but aims to develop Finland into a Global Data Hub. For this reason, Finland was one of the main investors in the C-Lion1 submarine cable project and it is also strongly supporting building of a cable between Asia and Europe.[182]

Digital sovereignty with regard to skills, norms and educational aspects

Are there specific 'seals' which promote DS?

Our research did not identify any such measures.

Are there (educational) programs to develop competencies, which promote DS?

The National Cyber Security Centre of Finland (NCSC-FI) offers situation awareness and collaboration management services in order to maintain and improve information security among citizens and organizations. [183]

Finnish Digital Innovation Hubs (DIH) contribute to the development of an innovative environment within which relevant start-ups and companies with acquire access to supporting and funding services. At the moment, there are 10 fully operational DIHs in Finland offering incubator / accelerator support and access to Funding and Investor readiness services.[184]

181 BCS North - Phase 1, BCS North - Phase 2, Baltic Sea Submarine Cable, C-Lion1, Eastern Light, Finland Estonia Connection (FEC), Finland-Estonia 2 (EESF-2), Finland-Estonia 3 (EESF-3) and Sweden-Finland 4 (SFS-4) , see https://www.submarinecablemap.com.

182 https://www.businessfinland.fi/en/do-business-with-finland/invest-in-finland/take-the-fast-track-to-finland/.

183 https://www.ncsc.fi/.

184 https://s3platform.jrc.ec.europa.eu/digital-innovation-hubs-tool?p_p_id=digitalinnovationhub_WAR_digitalinnovationhubportlet&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&formDate=1588943727740&freeSearch=&countries=25&evolStages=3&servicesProvided=10&servicesProvided=13&h2020=false.

7.10 Digital sovereignty in France

France is clearly one of the biggest actors to push DS; it is a declared goal by French policy makers. France is the second largest contributor to the GAIA-X project. Once more, France plans to apply stricter selection criteria for vendors for core parts in 5G networks and to exclude vendors such as Huawei.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

France has a very broad understanding of digital sovereignty. The focus is not only on economic arguments, but digital sovereignty is seen as an important sub-area and at the same time a prerequisite for national sovereignty. Digital sovereignty is also intended to defend the country's own social model and European values such as freedom, tolerance and solidarity. According to the French understanding, digital sovereignty is not only a task of the state, but also the task of the civil community.

France published a White Paper on Defence and National Security, which was presented by the President in June 2008. This noted that "*information systems security emerged, alongside deterrence, as an area in which the sovereignty of France should be fully expressed*." [185]

Digital sovereignty is a declared important sub-goal of the "Digital France" Project initiated by the Macron administration. However, France does not yet have an explicit Digital Sovereignty strategy. There was a commission of enquiry in the French Senate on the topic of "Digital Sovereignty", which presented its comprehensive report at the end of 2019. In this report, recommendations were made for the development of a strong digital sovereignty. Among other things, it recommends the development of a national strategy for digital sovereignty.[186]

With regard to Digital Sovereignty, the national cyber-security strategy is also an important component. The most recent version dates from 2015 (first version dates from 2011). A national agency for defence against cyber attacks was already established in 2009 (so called Agence nationale de la sécurité des systèmes d'information (ANSSI)[187]. ANSSI deploys a broad range of regulatory and operational activities, amongst other things issuing regulations and verifying their application. ANSSI reports directly to the Secretariat-General for National Defence and Security (Secrétariat général de la défense et de la sécurité nationale (SGDN)) [188] . SGDN is an interministerial organ under the Prime Minister of France. This symbolizes the high importance of cybersecurity and digital sovereignty within the French government.

---

185 French White paper on Defence and National security, June 2008, see https://www.cfr.org/content/publications/attachments/Dossier_de_presse_LBlanc_DSN_en_anglais.pdf.
186 http://www.senat.fr/commission/enquete/souverainete_numerique.html.
187 https://www.ssi.gouv.fr/en/.
188 http://www.sgdsn.gouv.fr/accueil/sgdsn-in-english/.

What is the approach towards DS?

France's approach to digital sovereignty has a strategic focus. The report of the Commission of Enquiry on Digital Sovereignty states that the cyberspace, far from the egalitarian utopia of its beginnings, has become a place of global confrontation, where struggles for influence, conflicts of interest and antagonistic social and economic logics take place. The reports states further that the digital revolution and the mastery of data have led to the emergence of economic players capable of competing with States. In the face of formidable competitors, the report comes to the conclusion that Digital Sovereignty is all about the question: "*How can an autonomous capacity for assessment, decision and action be maintained?*" This shows that France's approach to digital sovereignty goes far beyond purely economic objectives.[189]

According to France's national cyber security strategy, the State is pursuing five main objectives in cyberspace:

- Ensuring France's freedom of expression and action as well as the security of its critical infrastructures in case of a major cyberattack.
- Protecting the digital lives of citizens and businesses and combat cybercriminality.
- Ensuring the education and training required for digital security.
- Contributing to the development of an environment that is conducive to trust in digital technology.

Promoting cooperation between MS of the European Union (EU) in a manner favourable to the emergence of a European digital strategic autonomy, a long-term guarantor of a cyberspace that is more secure and respectful of European values.[190]

Digital sovereignty and technological aspects

In 2013 the "Critical Infrastructures Information Protection"-law (CIIP) was established. The law was proposed with the aim of establishing a common minimum level of cybersecurity for all critical operators. The law is destined to apply to more than 200 public and private operators from 12 sectors already identified as critical in France.[191]

The security rules defined in the CIIP-law are preventive actions aiming at reducing the risks of success for most cyberattacks. The rules were defined taking into account existing international standards.

Within the CIIP law, ANSSI shall be notified by operators of incidents occurring on their critical information systems. Furthermore, ANSSI can trigger security inspections done by its services, another State authority or a Trust Service Provider on a regular basis or following an incident. In case of a major crisis, declared by the Prime Minister, ANSSI

189 ANSSI, Information systems defence and security, France's strategy. See https://www.ssi.gouv.fr/publication/la-strategie-de-la-france-en-matiere-de-cyberdefense-et-cybersecurite/.
190 La stratégie de la France en matière de cyberdéfense et cybersécurité (2015), p. 9.
191 https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/.

can impose further measures. It lays down legal basis for action in the framework of crisis management plans.[192]

Are there selection criteria for hardware / software vendors?

According to media reports, France's cybersecurity agency ANSSI is currently developing a strategy to apply stricter selection criteria for vendors for core parts in 5G networks and to exclude so called high-risked vendors. For non-core parts, high risk vendors should continue to be available. It is expected, however, that similar to the UK strategy, certain exceptions will be defined, such as the exclusion of high-risk vendors from sensitive geographic locations, such as nuclear sites and military bases.[193]

The cybersecurity strategy states that 5G & Digital Sovereignty is on the government's agenda and that care will be taken to ensure the privacy and resilience of the 5G-networks through necessary adjustments to the regulatory framework. However, these measures are not defined in more detail. It is merely stated that "*France will remain attentive to the type and capabilities of equipment and software installed within these electronic communication networks, to protect the privacy of correspondences, that of its citizens and the resilience of these infrastructures*."[194]

Are there discussions on other technology aspects with an impact on DS?

In November 2018, the French government announced a strategy to support research development in the field of artificial intelligence. The aim is also to invest in state-of-the-art infrastructures and in the training of doctoral students. Finally, R&D cooperation with the European Member States, and Germany in particular, is to be supported in order to be able to compete with China and the USA.[195]

French Finance Minister Bruno Le Maire announced in 2019 that leading French companies Dassault and OVH would develop plans for entering the cloud services market in order to reduce the dependency on US cloud services like AWS, Microsoft and Google.[196]

Furthermore, France is the strongest supporter of the German GAIA-X Project. On February 18, 2020 a joint position paper on the GAIA-X project was published (Franco-German Position on GAIA-X)[197]. It postulates that the goal of the project is to facilitate the creation of European data and AI driven ecosystems, to guarantee data sovereignty, and to ensure that value creation remains with the individual participants. These ecosystems will focus initially on a number of sectors, including Mobility, Finance, Health, Living, Environment-Climate-Agriculture, Public Services and Industry 4.0. Projects on GAIA-X shall represent European values. It is therefore expected that all projects on GAIA-X are consistent with European ethical consideration for AI, as well as implement the highest level of data protection, security, transparency and portability /

192 https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/.
193 https://www.rcrwireless.com/20200313/5g/france-likely-allow-huawei-non-core-parts-5g-networks-report.
194 La stratégie de la France en matière de cyberdéfense et cybersécurité" (2015), p. 15.
195 https://www.europe1.fr/technologies/le-gouvernement-annonce-son-plan-pour-la-recherche-en-intelligence-artificielle-3809669.
196 https://www.atlanticcouncil.org/blogs/new-atlanticist/waving-the-flag-of-digital-sovereignty/.
197 Bundesministerium für Wirtschaft und Energie (2020): "Franco-German Position on GAIA-X".

reversibility. It's the aim of the project to strengthen the European position in a global digital market: "*In order to gain sustainable digital sovereignty, it is important to strengthen Europe's competitiveness in the global digital market.*"[198]

Digital sovereignty with regard to skills, norms and educational aspects

Are there specific 'seals' which promote DS?

France's cyber-security agency ANSSI has established the qualification of private "Trust Service Providers". Based on the provisions of the CIIP-law (for CIIP-law see above), an evaluation process allows the qualification of candidates providers meeting the adequate security and trust requirements.

These providers are qualified on the basis of reference documents established by ANSSI after public consultations and trial phases. The qualification process includes the assessment of the skills of each consultant and the solidity of the companies.[199]

Are there (educational) programs to develop competencies, which promote DS?

Our research did not identify any such measures.

198 Ibid, p. 1.
199 https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/faq/.

7.11 Digital sovereignty in Germany

Germany is the main contributor to the GAIA-X project. Germany's federal government has obligations to use information technology "Made in Germany" and so called "focus groups" set by the Ministry of Economic Affairs are strong contributors to the political discussion of DS. However, Germany is less restrictive while reviewing high risk suppliers for its 5G networks.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

Digital sovereignty was first defined in the paper "Guardrails of Digital Sovereignty" by the focus group "Digital Sovereignty" of the Federal Ministry for Economic Affairs and Energy in 2015. In the paper, being sovereign is defined as being capable of self-determined actions and decisions without relying exclusively on one's own resources. This means that business, science and society can use (digital) products, services, platforms and technologies in such a way that, for example, their own security or data protection interests are not impaired, that no inevitable dependencies arise and that their own business ideas and models can be realised. Digital sovereignty also means that business, science (and in some cases public administration) are in a position to develop digital technologies, bring them to market and distribute them nationally and internationally.[200]

For the federal government's Digital Summit in 2018 in Nuremberg, the paper "Digital Sovereignty and Artificial Intelligence – Prerequisites, Responsibilities and Recommendations for Action" upgraded the importance of the topic of digital sovereignty by expanding it from a technological or economic dimension to a general socio-political relevance. With the federal government's cloud project "GAIA-X", designed as a hyperscaler, which was presented at the 2019 Digital Summit in Dortmund, the topic of digital sovereignty was brought into the consciousness of the general public.

The ministries involved in digitalisation and digital sovereignty are the Federal Ministry for Economic Affairs and Energy, especially concerning the realization of Industry 4.0, and the Ministry of Transport and Digital Infrastructure.

What is the approach towards DS?

The German government is pursuing a very broad approach to digital sovereignty. In addition to considering individual economic and technological areas, Germany also believes that digital sovereignty must be based on social and ethical principles. This socio-ethical foundation is seen in the European tradition of humanism. Oriented towards universal basic rights and human dignity, digital sovereignty should guarantee values such as freedom, respect and tolerance. Digital sovereignty is therefore seen as a means of defending and maintaining one's own political and social system. Digital

200 Federal Ministry for Economic Affairs and Energy. 2015. Leitplanken Digitaler Souveränität. Presented at the National IT Summit 2015.

sovereignty is interpreted as an important sub-aspect of general sovereignty, which includes the ability for independent self-determination with regard to the use and design of digital systems themselves, the data generated and stored in them, and the processes they represent.

According to the understanding of the German government, the digital sovereignty of a state or an organization necessarily includes complete control over stored and processed data as well as the independent decision on who may access it. It also includes the ability to independently develop, modify, control and supplement technological components and systems with other components.[201]

How is DS translated into practical measures?

A study published in 2019 on behalf of the Federal Ministry of the Interior, Building and Community titled "Strategic market analysis to reduce dependencies on individual software providers" underpins the increasingly critical technology dependence of public administration in Germany. Following this, the respective minister announced that "*to ensure our digital sovereignty, we want to reduce our dependencies on individual IT providers. We are also examining alternative programs to replace certain software*." Open source software will also play an important role, the ministry states.[202]

Germany has also tightened regulations concerning foreign direct investments from non-EU/EFTA entities in critical infrastructure, such as energy, water, telecommunications and defence. Investors in sectors including media, artificial intelligence, robotics, semi-conductors, biotechnology and quantum technology, would have to make public any purchases of 10% voting rights or more and allow the German government to review them.[203]

Further measures for the Federal Government and Federal Administration are the encryption of wired electronic communication with SINATechnology, secure mobile communication with smartphones and tablets through the solutions SecurePIM (iOS), SecuSuite (Android, BlackBerry) and SINA (Windows, Linux).

Digital sovereignty and technology

Are there selection criteria for hardware vendors in general?

The strategy paper "Digital Sovereignty and Artificial Intelligence – Prerequisites, Responsibilities and Recommendations for Action" by the "Digital Sovereignty Focus Group", an ICT-expert team supervised by the German Federal Ministry for Economic Affairs and Energy, sets some general guidelines on this. According to the paper, the first basic requirement for reliable digital infrastructures is trustworthy technology. All

201 Fokusgruppe „Digitale Souveränität in einer vernetzten Gesellschaft" (2018): „Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen" (2018), p. 3 in combination with Deutscher Bundestag (2019).

202 https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2019/09/digitale-souveraenitaet-oeff-verwltg.html.

203 For more information, see https://www.bakermckenzie.com/en/insight/publications/2019/01/germany-widens-the-scope. For an English version of the specific law, see Foreign Trade and Payments Ordinance (Außenwirtschaftsverordnung - AWV): Division 2 Examination of corporate acquisitions https://www.gesetze-im-internet.de/englisch_awv/englisch_awv.html#p0508.

active components that ensure the transport of data in the digital (mobile) networks must have the highest degree of trustworthiness. They must ensure that the data takes the right route, reaches its intended recipient, is not tapped and is not manipulated[204].

Furthermore, the German Federal Network Agency, the regulatory office for telecommunication, states that security-related network and system components (critical key components) may only be used following an appropriate acceptance test upon supply and must be subjected to regular and ongoing security tests[205]. At present, together with the Federal Office for Information Security and the Federal Commissioner for Data Protection and Freedom of Information, the network agency is revising the respective and legally binding catalogue of security requirements for the operation of telecommunications networks and data processing systems and for the processing of personal data.

According to the German "Digital Sovereignty Focus Group", for 5G, Europe still has a real opportunity to develop, together with the European infrastructure manufacturers, its own service provision that will allow European network operators to build a trustworthy 5G infrastructure. Yet, for Germany itself, where Huawei is a provider of core parts to telecoms operators, "*a ban is not an option*", Chancellor Angela Merkel said at the Global Solutions summit in Berlin (March 2019)[206]. The favoured approach consists of mitigating security risks by setting additional security requirements, e.g. the use of critical key components being made subject to certification.

As for the ongoing revision of security requirements set by the German Federal Network Agency, new rules for the operation of telecommunications networks and data processing systems and for the processing of personal data are planned. In particular, for operators of public telecommunications networks with a high potential threat, security requirements are to be specified that must be complied with when determining the appropriate technical measures or other safeguards. The following additional security requirements are planned:

- *"Systems may only be sourced from trustworthy suppliers whose compliance with national security regulations and provisions for the secrecy of telecommunications and for data protection is assured"*; and
- "*Network traffic must be regularly and constantly monitored for any abnormality and, if there is any cause for concern, appropriate protection measures must be taken*".[207]

---

204 „Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen" (2018), p. 3 in combination with Deutscher Bundestag (2019).

205 BNetzA Press Release March 2019 "Bundesnetzagentur publishes key elements of additional security requirements for telecommunications networks"; for the catalogue on safety requirements, see: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen.pdf?__blob=publicationFile&v=7.

206 See, for example: https://www.bloomberg.com/news/articles/2019-03-19/merkel-takes-a-stand-against-u-s-pressure-to-bar-huawei-from-5g.

207 BNetzA Press Release March 2019 "Bundesnetzagentur publishes key elements of additional security requirements for telecommunications networks".

However, the agency's president also notes in a press release that the "*[s]ecurity requirements apply to all network operators and service providers, irrespective of the technology they deploy. All networks, not just individual standards like 5G, are included*."[208]

Are there discussions on other technology aspects with an impact on DS?

Germany's Cloud project: The German federal government has initiated the cloud project "GAIA-X", which is aimed to connect centralised and decentralised infrastructures in order to turn them into a homogeneous, user-friendly system. According to the initiators, the resulting federated form of data infrastructure is supposed to strengthen both the digital sovereignty of cloud service-users and the scalability and competitiveness of European cloud-service providers. First test of the technical concept are planned for the second quarter of 2020, live operations are planned to start by the end of 2020 with the first service-providers and users[209]. The background of this project is the strategic importance of cloud services. For the cloud market in the context of AI for example, it is argued that US and Chinese providers dominate all three stages of the cloud market value chain. At the infrastructure level [IaaS], which provides computing and storage capacity, US providers dominate the global market. However, the higher platform level [PaaS] and the software level [SaaS] are also dominated by a few providers, with the result that platform-independent applications (so-called middleware with open interfaces between infrastructure and software) are increasingly being displaced.[210]

Digital sovereignty with regard to skills, norms and educational aspects

Are there specific 'seals' which promote DS?

In June 2020, Germany announced a €20 million "Trustworthy Electronics" programme to boost home-grown electronics. Research Minister Anja Karliczek noted on this initiative that "*Germany is a country of innovation and wants to remain that [way]. It is important that we assert ourselves in international competition with key technologies and are technologically sovereign*,"[211]

Are there (educational) programs which develop competencies, which can promote DS?

In Germany there are several programs aiming to develop general digitalisation or specific areas, like "Designing digitization"[212] and the "Artificial Intelligence Strategy"[213].

---

208 BNetzA Press Release March 2019 "Bundesnetzagentur publishes key elements of additional security requirements for telecommunications networks".

209 Federal Ministry for Economic Affairs and Energy. 2019. Project GAIA-X - A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem.

210 Federal Ministry of Economic Affairs. 2018. Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen. Presented at the National IT Summit 2018.

211 https://sciencebusiness.net/news/tech-sovereignty-rises-eu-agenda-germany-launches-homegrown-electronics-programme.

212 https://www.bundesregierung.de/resource/blob/975226/1552758/c34e443dbe732e79c9439585b4fbade5/pdf-umsetzungsstrategie-digitalisierung-data.pdf?download=1.

213 https://www.de.digital/DIGITAL/Redaktion/EN/Standardartikel/artificial-intelligence-strategy.html.

Beside more general goals as strengthening digital education and training and generating knowledge and innovations from data the Digital Strategy of the Federal Ministry of Education and Research of 2019 has specified as one of its aims to "*ensure technological sovereignty and scientific leadership*".[214]

214 https://www.bildung-forschung.digital/files/BMBF_Digitalstrategie_web.pdf.

7.12 Digital sovereignty in Greece

Greece, mainly due to its low level in overall digitalization, has a very narrow definition of DS as it is practically not on the agenda at all. A project which stands out is GRNET, a government own company with the mission to provide high-quality infrastructure and services to the academic, research and educational community of Greece, and to disseminate ICT to the general public.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

Digital sovereignty is not on the agenda of the government of Greece. However, aspects of the digitalization strategy may be seen as moves towards digital sovereignty.

What is the approach towards DS?

The approach of the country is merely focused on general digitalisation. The National Digital Strategy is the road map and framework supporting the country's digital development. According to the National Digital strategy, the relevant public entities have to implement a National Cyber Security Strategy which will define the strategic objectives and specific policy actions that must be implemented.[215]

How is DS translated into concrete political and regulatory measures?

Merely as cybersecurity strategy.

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors in general?

There are no official publications regarding security guidelines so far, however there are discussions regarding 5G vendors in the Greek market.

Huawei ran a pilot 5G program in Kalamata, in the Peloponnese, with Greek telecom provider Wind Hellas in the summer of 2019. Beside resistance due to health concerns, there were signals that the US put pressure on Greece as well in this matter. President Donald Trump met begin January 2020 with Greek Prime Minister Kyriakos Mitsotakis in Washington, but formal confirmation om this topic was not given.[216]

Is there a discussion on other technology aspects with an impact on DS?

Greece seems to align with major EU coordinated programs with an impact on digital sovereignty; In May 2020, Greece signed the Declaration on cooperation on Artificial Intelligence and it is also a member of the EuroHPC Joint Undertaking.

---

215 https://mindigital.gr/old/images/GENIKOI/RALIS/PDF/Digital_Strategy_2016_2021.pdf.
216 https://greece.greekreporter.com/2020/01/10/greece-appears-to-bow-to-us-pressure-delays-decision-on-chinese-5g-network/.

Digital sovereignty with regard to skills, norms and educational aspects

Are there specific 'seals' which promote DS?

There is a data protection certificate for cloud computing services hosting public services.[217]

Are there (educational) programs to develop competencies which can improve DS?

In Greece there are no specific educational programmes that aim to raise awareness on digital sovereignty, however there are initiatives aiming to enhance the digital skills of individuals. Such initiatives are the establishment of the "Greek National Coalition[218] on Digital Skills and Jobs" and the implementation of actions within the framework of the "New Skills Agenda" of the European Commission have been a key priority for the past few years[219]. The available educational programmes are mainly focused on smart specialization and are provided in the framework of General Secretariat for Research and Technology (GSRT).[220]

217 https://mindigital.gr/old/images/GENIKOI/RALIS/PDF/Digital_Strategy_2016_2021.pdf.
218 http://elke.eap.gr/wp-content/uploads/2018/07/dsgr_action_plan_eng_subm4_no-memo.pdf.
219 https://www.nationalcoalition.gov.gr/en/history_en/.
220 http://www.gsrt.gr/central.aspx?sId=120I466I1396I323I496367.

7.13 Digital sovereignty in Hungary

Hungary's scope of DS ranks medium. The protection of Hungary's sovereignty in its cyberspace is a national interest. A free, democratic and secure functioning of the Hungarian cyberspace based on the rule of law is regarded as a fundamental value and interest.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

Aspects of digital sovereignty can only be found in the national cybersecurity strategy. The National Cyber Security Strategy of Hungary (NCSS) was adopted in 2013, which makes Hungary one of the first Central European countries to formulate one. The strategy is "*based on the foundations of EU and NATO cybersecurity principles and follows the mainstream take on cybersecurity strategies (values, environment, objectives, tasks, and tools)"*.[221]

What is the approach towards DS?

For Hungary, only a more general approach towards digitalization can be described. However, some of these aspects contain themes of digital sovereignty. For example, "*flagship digital multinationals have decided to bring new investment projects to Hungary*", referring to investments by Bosch, Mercedes-Benz and SAP. The minister of Foreign Affairs and Trade added that "*Bosch and component maker ZF are also in the process of launching engineering investment projects, preparing the ground for technologies to be applied in the electro-mobility sector, including the manufacture of self-driving cars".*[222]

How is DS translated into concrete political and regulatory measures?

Again, only general digitalization aspects can be described for Hungary. Hungarian Government has applied another regulatory measure by fostering the region's best investment environment by creating the most efficient way to link production through digitization. "*Hungary aims to become one of Europe's most competitive bases for research and development".* Furthermore, "*the car industry and the transition to new technology continue to play leading roles in Hungary's economy*", and "*several development centres are being set up for autonomous vehicles in Hungary and special attention is being paid to expanding the base of Hungarian suppliers".*[223]

221 https://www.cyberwiser.eu/hungary-hu.
222 http://abouthungary.hu/news-in-brief/fm-hungary-has-been-successful-in-transforming-its-economy-to-adapt-to-the-digital-age/.
223 http://abouthungary.hu/news-in-brief/hungary-aims-to-become-leading-research-and-development-hub/.

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors in general?

As for the handling with Huawei, Hungary's government has said it had no evidence that the Chinese company's equipment would pose a security threat: "*Foreign Minister Peter Szijjarto announced at an event in China that Hungary would involve Huawei in the 5G rollout."*

The responsible Minister of Foreign Affairs and Trade said that Huawei would cooperate with Vodafone and Deutsche Telekom in the Hungarian build-up. However, Deutsche Telekom's Hungarian unit said Huawei was just one of the suppliers tested for the 5G technology.[224]

Is there a discussion on other technology aspects with an impact on DS?

Hungary has an AI strategy, which is aimed at contributing to its economy and in such is not directly DS. [225] Furthermore, there are efforts to increase the use of cloud computing services in the same context. [226]

Digital sovereignty with regard to skills, norms and educational aspects

Are there 'seals' which promote DS?

Our research did not identify any such measures.

Are there (educational) programs to develop competencies for DS?

There are multiple general development programs from the Hungarian government to enhance digital skills, however this can't directly be labelled as DS.[227]

224 https://www.reuters.com/article/us-hungary-telecoms-huawei/hungarian-minister-opens-door-to-huawei-for-5g-network-rollout-idUSKBN1XF12U.
225 https://ec.europa.eu/knowledge4policy/ai-watch/hungary-ai-strategy-report_en.
226 https://bbj.hu/business/clouds-of-data-over-europe_63447.
227 http://abouthungary.hu/news-in-brief/pm-orban-creates-schemes-to-promote-digital-education/.

7.14 Digital sovereignty in Ireland

DS is not on the political agenda in Ireland and aspects of it can only be found in the cyber security strategy. Regarding the language towards US technology companies, Ireland seems to be very careful as most of them companies have their European headquarter in Ireland and their tax impact weighs heavily on Ireland's policy makers.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

Ireland launched the National Digital Strategy "Phase 1 – Digital Engagement" in 2013 with the main focus to get its citizens and business online. Building on this, the Irish government is currently developing a new National Digital Strategy to further embrace the opportunities that come with digitalisation, but also to address its challenges.[228] "Digital Sovereignty" was not subject of this strategy.

A public consultation on the national digital strategy was launched on 22 October 2018, where members of the public as well as stakeholders could make submissions. The consultation is currently under review.[229] The development of a new National Digital Strategy is being led as a shared effort by the Department of the Taoiseach; Department of Communications, Climate Action and Environment; Department of Business, Enterprise and Innovation, and the Office of the Government Chief Information Officer in the Department of Public Expenditure and Reform. Accordingly, the new strategy will range from a variety of fields: Societal and economic areas including, infrastructure and security; data, privacy and regulation; education and skills; trust, wellbeing and inclusion; digital public services, and innovation, the digital economy, and labour market changes.[230]

The National Broadband Plan of 2012 does not address any issues of sovereignty nor promotes the use of Irish or EU solutions. The main focus is to ensure fast connectivity.

What is the approach towards DS?

The first National Cyber Security Strategy, agreed by Government in 2015, set out a series of measures that would be taken to build the capability of the National Cyber Security Centre and to achieve a high level of security for computer networks and critical infrastructure in the State. The Strategy also established how the resilience of critical national infrastructure would be improved, in part by the transposition of the EU Network and Information Security Directive.[231]

It should also be stated that most of the international IT companies (which, among others, include US companies Apple, Microsoft, Alphabet, Intel, IBM and Facebook)

228 https://www.dccae.gov.ie/en-ie/communications/topics/Digital-Strategy/Pages/default.aspx.
229 https://www.gov.ie/en/consultation/1618101010-national-digital-strategy/.
230 https://www.gov.ie/en/press-release/69baa0-government-seeks-views-on-irelands-digital-strategy/.
231 https://www.dccae.gov.ie/en-ie/news-and-media/press-releases/Pages/National-Cyber-Security-Strategy-published.aspx.

have their European headquarters in Ireland. Hence, a strong stance against US technology is not expected.

How is DS translated into practical measures?

The National Cyber Security Centre has worked, on an ongoing basis, with utility operators and with similar bodies in other jurisdictions to ensure that risks to infrastructure in Ireland are managed appropriately, including the active management of ongoing issues.

ComReg (NRA) sub unit "Network Operations Unit" monitors and ensures providers' compliance for network resilience and security.[232] ComReg also has power in respect of data privacy.

Digital sovereignty and technology

Are there selection criteria for hardware / software vendors?

In the context of accusations of industrial espionage by Huawei from the US, the chief executive of Eir, Ireland's biggest telecommunications company told newspapers in January 2020, that Eir is "*happy with Huawei*" and will continue to order radio access equipment from Huawei while the "*more sensitive*" core network equipment is being supplied by Sweden's Ericsson.[233] Vodafone has teamed up with Ericsson as it gears up to launch 5G capability by the end of this year and doesn't use Huawei equipment, while Three Ireland has previously said it does not use Huawei equipment.[234]

In December 2015 the program *Considering Cloud Services* was issued in line with the Public Service ICT Strategy. It provided advice to assist public service organisations in making informed, risk-based decisions in relation to the adoption of cloud services.[235] As most of this advice is still valid, in 2019, the Department of Public Expenditure and Reform published a renewed version. In the 2019 advice, it is stated that in general cloud computing services should be considered potentially suitable for any category of public service information or system except where such data would be classified as 'top secret'. Consequently, all new government systems should be developed to exploit the opportunities presented by cloud deployment, where possible and all existing systems will be reviewed for cloud capability. Systems should move to public cloud or government private cloud environments over time and where practicable.

232 https://www.comreg.ie/publication-download/network-operations-annual-report-2018.
233 https://www.irishtimes.com/business/technology/eir-very-happy-with-huawei-as-supplier-for-5g-network-1.4153946.
234 https://www.irishtimes.com/business/technology/huawei-tech-not-included-in-core-networks-of-irish-5g-operators-1.3923330.
235 https://www.gov.ie/en/consultation/1005021610-advice-note-considering-cloud-services/.

Digital sovereignty with regard to skills, norms and educational aspects

Are there (educational) programs which promote DS?

Mainly cybersecurity related:

In 2012, the Department of Communications, Climate Action and Environment, in partnership with industry sponsors, re-launched the “Make-IT-Secure” campaign, which informs small and medium sized businesses and the general public about steps they can take to improve their cyber security. Cork Institute of Technology (CIT), supported by the IDA, have established a programme to establish and grow a Cyber Security Cluster in Ireland. The cluster will include stakeholders from industry, academia and government and will seek to encourage co-operation, raise awareness of education and career opportunities, drive innovation and stimulate new business in the Cyber Security field.[236]

236 https://www.cit.ie/currentnews?id=1388.

7.15 Digital sovereignty in Italy

Italy does not have DS directly on its agenda. DS aspects are only found in their cyber security strategy. Italy has also developed a national cloud and databases of national interest.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

Strategies merely focused on general digitalisation, like the Italian Digital Agenda. In addition the ministry of innovation has recently published a national plan 2025, a strategy paper for technological innovation and digitization of the country.[237] According to a newspaper article, digital sovereignty is linked to data protection and data integrity and cloud infrastructures have a key strategic role.[238]

What is the approach towards DS?

Only strategic plans found for digitalisation in line with the European Digital Agenda (so focused on access and coverage of broadband).

How is DS translated into concrete political and regulatory measures?

The Three Year Plan for IT in Public Administrations 2017-2019 introduced the PA Cloud Model that describes the set of IT infrastructures and cloud services qualified by the Agenzia per l'Italia Digitale (AgID) at the PA's disposal.[239]

A Cybersecurity Decree has been adopted in November 2019.[240] It extends special powers of the Government (the so-called Golden power), which are also extended to 5G. Bilateral agreements between countries must ensure that safety standards are met.

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors in general?

According to the Piano Triennale, the infrastructures that provide cloud services need to be qualified by AGID (Agenzia per l'Italia Digitale). For example, the Cloud Software provider (SaaS) has to declare to be certified according to the ISO/IEC 27001 standard extended with the controls of ISO/IEC 27017 and ISO/IEC 27018.

The certification must have been issued by national accreditation bodies recognized by the European Union.[241] In case of location of the datacenters in non-EU territory, 2016

237 https://innovazione.gov.it/assets/docs/MID_Book_2025.pdf.
238 https://www.agendadigitale.eu/sicurezza/privacy/sovranita-digitale-le-mosse-dei-paesi-ue-e-perche-e-una-pericolosa-deriva/.
239 https://www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_linformatica_nella_pubblica_amministrazione_2019_-_2021_allegati20190327.pdf.
240 https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg and https://www.repubblica.it/politica/2019/11/13/news/cybersicurezza_legge-241041589/.
241 https://cloud-italia.readthedocs.io/projects/cloud-italia-circolari/it/latest/circolari/CSP/allegato_docs/requisiti-specifici.html#sicurezza-privacy-e-protezione-dei-dati.

regulation obliges that a SaaS supplier declares the possible applicability of bilateral agreements aimed at safeguarding the data processed, stored and in various ways managed to provide the service.

Moreover, the Department of Information for Security (Dis) has provided a 'cybernetic security perimeter' to give concreteness to the digital borders to be protected, integrating public and private structures.[242]

A Cybersecurity Decree has been adopted in November 2019.[243] It extends special powers of the Government (the so-called Golden power), which are also extended to 5G. The decree provides for new measures on Cybersecurity by establishing the National Cyber Security scope. In particular, the decree extends the veto power also over companies holding strategic assets.[244] It will be the Presidency of the Council and no longer the Agency for Digital Italy to carry out the activities of inspection and verification of compliance with the adoption of rules to protect security by public subjects, while the Ministry of Economic Development remains responsible for private subjects. In October 2020, the Italian government vetoed a 5G cooperation between operator Fastweb and supplier Huawei.[245]

With regards to 5G the rules apply to entities included in the national cyber-security scope, including contracts or agreements with entities outside the European Union - relating to broadband electronic communications services based on 5G technology. A notification to the Presidency of the Council is required for the possible exercise of power or imposition of specific requirements or conditions.

Purchases by parties/companies outside the EU are subject to notification to the Government. Moreover companies that hold specific assets and relationships, including infrastructure and critical technologies related to data management and Cybersecurity are subject to notification to the Government.[246]

Are there discussions on other technology aspects with an impact on DS?

For databases of 'national interest', there are not only quality requirements (defined by the data quality standard ISO/IEC 25012 Data quality model[247]), but also technical rules as defined by AGID with Determination n. 68/2013 for critical databases.[248]

242 https://www.affarinternazionali.it/2020/01/sovranita-digitale-priorita/.
243 https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg and https://www.repubblica.it/politica/2019/11/13/news/cybersicurezza_legge-241041589/.
244 https://www.repubblica.it/politica/2019/11/13/news/cybersicurezza_legge-241041589/.
245 Telecoms.com, 26 October 2020, see https://telecoms.com/507100/italy-reportedly-blocks-huawei-5g-deal-as-bulgaria-joins-us-clean-network-scheme/.
246 https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg.
247 https://www.iso.org/obp/ui/#iso:std:iso-iec:25012:ed-1:v1:en.
248 https://www.agid.gov.it/sites/default/files/repository_files/circolari/dt_cs_n.68_-_2013dig_-regole_tecniche_basi_dati_critiche_art_2bis_dl_179-2012_sito.pdf.

Digital sovereignty with regard to skills, norms and educational aspects

Are there (educational) programs which promote DS?

Under the flag of 'Republica Digitale', there is a national strategic initiative pushing for digitalisation. It is promoted by the Department for Digital Transformation of the Presidency of the Council of Ministers with the aim of, among others, combating the digital divide in the Italian population.[249] Furthermore, there is the "Italy 2025" strategy, with similar goals. [250]

No specific programs promoting digital sovereignty.

249 https://innovazione.gov.it/it/repubblica-digitale/.
250 https://www.tuv.it/it-it/campaigns/blog/innovazione-e-digitale/smart-working-misuriamo-le-performance-per-un-miglioramento-efficace.

7.16 Digital sovereignty in Latvia

Cybersecurity is the key component of DS in Latvia. Latvia calls for a EU-blacklist of 5G vendors and does not want to single-handedly exclude any vendors.

Digital sovereignty in general

How is Digital Sovereignty defined in the respective country?

Only the cybersecurity dimension; "*Latvian state administration, society and economy depend on the opportunities and services ensured by information and communication technology […]*". Cybersecurity policy has been applied in order to achieve a *"secure and reliable national cyber space, which ensures a safe, reliable, and continuous supply of services essential for the state and society"*[251].

Is digital sovereignty (DS) on the agenda of the government?

"*Cyber security policy implementation in Latvia involves a broad, comprehensive range of interested parties, […]"*. The implementation applies, among others on critical Infrastructure, "*for the performance of basic functions essential for state and society to ensure the integrity, accessibility and confidentiality*"[252].

What is the approach towards DS?

Not clear. Most of the approaches directed at improving digitalisation and related skills as "*Latvia invested just 0.6% of GDP in R&D in 2015, while the share of venture capital investment in the ICT sector in 2016 was well below that in other European countries*"[253].

> On 17 September, Cabinet of Ministers approved the informative report 'Cyber Security Strategy of Latvia for 2019-2022' presented by Ministry of Defence. The strategy describes cyber security context of Latvia, identifies future challenges and national cyber security policy priorities. […] To achieve its objective, policy proposes actions in five areas: enhanced cyber security and manageable digital security risks; resilience of ICT systems; better universal access to strategic ICT systems and services; public awareness, education and research; international cooperation; rule of law in cyber space and cyber-crime prevention.
>
> According to the Strategy, Ministry of Defence and other competent authorities will have to complete specific tasks, for example, define security standards for cloud computing, smart devices and on-line services […][254].

---

251 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/latvian-national-cyber-security-strategy, Latvian National Cyber Security Strategy.

252 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/latvian-national-cyber-security-strategy, Latvian National Cyber Security Strategy.

253 https://www.oecd.org/policy-briefs/Latvia-digitalisation.pdf.

254 https://www.mod.gov.lv/en/news/latvia-approves-new-cyber-security-strategy-2019-2022.

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors in general?

Our research did not identify any such measures.

Is there a discussion on other technology aspects with an impact on DS?

There is a focus on AI with parties like the the Artificial Intelligence Laboratory (AiLab) researching part-of-speech tagging and user-generated content in news portal communities. [255] For example Latvia has the first AI news anchor in Europe, a female character named Laura reading the *"news in Latvian using the latest deep machine-learning techniques. […] Up to now, only Google and Baidu have been able to implement this approach for a limited number of languages*."[256].

Are there discussions specifically on 5G vendors?

> In July 2019, Latvia became one of the first countries in Europe [to introduce] 5G network coverage. […] 5G was introduced in Latvia by "Latvian Mobile Telephone" (LMT), one of the most ambitious and innovative companies in Latvia with more than 25 years of experience in the telecommunication sector[257].

Security guidelines have been introduced by LMT including mission management system, drone traffic management, and computer vision. Its implementation will be done by LMT's potential clients.[258]

Latvia and the United States on February 27 signed a "Joint Declaration on 5G Security" [259] . This effectively aligns Latvia's future development of its 5G communications networks with the U.S. approach to avoiding using high risk vendors in vital parts of 5G networks.[260]

Digital sovereignty with regard to skills, norms and educational aspects

Are there (educational) programs which develop competencies to promote DS?

Our research did not identify any such measures.

---

255 http://www.digitalhumanities.lv/institutions/ailab/.
256 https://www.itbaltic.com/single-post/2019/03/27/Artificial-intelligence-is-the-new-black-in-digital-transformation-for-media-around-the-globe.
257 https://china-cee.eu/2020/01/22/latvia-political-briefing-latvia-5g-pioneer-in-the-north-of-europe/.
258 https://china-cee.eu/2020/01/22/latvia-political-briefing-latvia-5g-pioneer-in-the-north-of-europe/.
259 https://eng.lsm.lv/article/politics/diplomacy/latvia-and-us-sign-declaration-on-future-of-5g-communications.a349593/.
260 https://www.state.gov/joint-statement-on-united-states-latvia-joint-declaration-on-5g-security/.

7.17 Digital sovereignty in Lithuania

Lithuania is only concerned with cyber security, hence its definition of DS is narrow. Lithuania also signed a declaration with the US which aligns their approach for the expansion of 5G.

Digital sovereignty in general

How is Digital Sovereignty defined in the respective country?

Digital Sovereignty of Lithuania is mainly defined in the National Cyber Security Strategy, which was adopted in 2011. It is a comprehensive plan that includes an assessment of Lithuania's cybersecurity capacity. The main objectives are ensuring the security of state-owned information resources, an efficient functioning of critical information infrastructure, and the Cyber security of Lithuanian residents and persons staying in the country.[261]

Is digital sovereignty (DS) on the agenda of the government?

The current Lithuanian Digital Agenda strategy, the Information Society Development Programme for 2014-2020 was adopted in 2014 and amended in December 2017. The strategy covers all areas of the digital economy and society: from digital skills to broadband coverage, e-government, use of open public data etc. This programme was complemented in August 2018 by a National Cybersecurity Strategy.[262]

What is the approach towards DS?

Main focus is on general digitalisation and bringing the benefits of ICT to its economy and citizens. No direct strategies or mentioning of digital sovereignty.[263]

The development of society in general is named in the Lithuanian Information Society Development Programme 2014-2020 "Digital Agenda of the Republic of Lithuania". It focuses on 3 major areas: 1) skills and motivation of the Lithuanian citizens to use ICT, 2) development of electronic content and 3) evolvement of ICT infrastructure, including NGA access.[264]

How is DS translated into concrete political and regulatory measures?

No clear measures aimed at digital sovereignty.

---

261 https://www.cyberwiser.eu/lithuania-lt.
262 https://ec.europa.eu/digital-single-market/en/scoreboard/lithuania.
263 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/programme-for-the-development-of-electronic-information-security-cyber-security-for-2011-2019-2011.
264 https://ec.europa.eu/digital-single-market/en/country-information-lithuania.

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors in general?

No general specific selection criteria. In the context of 5G, there are discussions and even proposals made at EU level (for a blacklist).

Is there a discussion on other technology aspects with an impact on DS?

> In the fall of 2018[265] an expert group met up with the Ministry of Economy of the Republic of Lithuania to discuss the impact of artificial intelligence technologies. […]
>
> The group consisted of industry leaders, academic experts and government representatives, all with knowledge on the Lithuanian AI ecosystem. A Landscape Report was released by the group in November of 2018 highlights [sic] both the key areas where Lithuania is successful in AI and where there is room for growth.

It follows as well the EU AI ethics standards, hence promoting European values within Lithuania's AI strategy.

Regarding 5G development, there is an issue that the 3.5 GHz radio frequencies for 5G are used for military radar by Russia in bordering Kaliningrad. The used signal "*seeps into parts of Lithuanian territory.*"[266].

Are there discussions specifically on 5G vendors?

In 2019, Lithuania was preparing to launch frequencies auction for its 5G network, and suggested to the European Commission "*to create a blacklist of companies, create a cyber security clause for equipment certification, and make sure that national security requirements are part of frequencies auctions' conditions*."[267].

Digital sovereignty with regard to skills, norms and educational aspects

Are there state 'seals of approval' showing a certain compliance and/or quality?

Our research did not find direct seals on DS but on cybersecurity; Law of the Republic of Lithuania on Electronic Identification and Trust Services for Electronic Transactions is the only seal of approval. The law's 10th article identifies the obligations of Trust Providers.[268]

In April 2019, the Ministry of Economy published a report on the Lithuanian Artificial Intelligence Strategy: A Vision of the Future. One of their policy recommendations was to "*incentivize companies that are forerunners of their sectors for AI implementation.*

---

265 https://medium.com/@alexmoltzau/lithuanian-artificial-intelligence-strategy-2019-919ded83cc86.
266 https://www.lrt.lt/naujienos/news-in-english/19/1054680/russian-military-a-barrier-to-5g-development-in-lithuania.
267 https://www.lrt.lt/en/news-in-english/19/1083147/lithuania-ready-for-5g-but-only-chinese-companies-can-provide-full-package.
268 https://e-seimas.lrs.lt/portal/legalAct/en/TAD/c5174772ecd011e89d4ad92e8434e309.

Companies can be granted an AI Badge that will publically position them as leaders in the field."[269].

Are there (educational) programs to develop competencies, which promote DS?

Lithuania seems not to have strong educational programs in respect to digital sovereignty. Furthermore, an OECD report notes Lithuania has almost the highest ranking (57%) in the EU in terms of risking that its labour force is being replaced by automation (with AI). Only in Slovakia, this risk is even higher.[270]

269 http://kurklt.lt/wp-content/uploads/2018/09/StrategyIndesignpdf.pdf.

270 Nedelkoska, L. and G. Quintini (2018), "Automation, skills use and training", OECD Social, Employment and Migration Working Papers, No. 202, OECD Publishing, Paris, https://doi.org/10.1787/2e2f4eea-en.

7.18 Digital sovereignty in Luxemburg

Luxemburg focuses on a digitalized nation including its important financial sector and datacentres. DS is based on cyber security, but the goal is clearly to protect ICT infrastructure in order to ensure the availability of essential services and economic interest. Hence, Luxemburg's scope of DS is medium.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

Merely the cybersecurity dimension of digital sovereignty; the new national cybersecurity strategy for 2018-2020 reflects that the government is aware of both the opportunities and risks which are inherent in new technologies. It is in this context that one of the main guidelines is about "*the protection of digital infrastructure, in order to ensure the availability of essential services […]*"[271].

What is the approach towards DS?

Luxembourg has undertaken an ambitious economic diversification strategy for the digital sector, called Digital Luxembourg, which was founded in 2014.[272] As stated in January 2020 by Étienne Schneider, Deputy Prime Minister and Minister of the Economy of Luxembourg, "*the government recognised at an early stage that the future lies in the digitalisation of our economy and society […] Our ICT infrastructure, capacities and competences are outstanding, and we have steadily maintained a high level of investment in the field […] Data centres, connectivity, cyber-security and related skills are at the heart of our strategy to be a trusted hub for valuable data. Luxembourg will strive to become the most trusted data economy within the European Union by 2023".* [273]

The Ministry of the Economy has mandated since 2010 the entity SECURITYMADEIN.LU, to promote and strengthen information security in Luxembourg.[274] Furthermore, the Ministry drives the innovation in the ICT sector together with Luxinnovation, the national agency for the promotion of innovation.[275]

In addition, there is an "Open data policy", which enables the (commercial) re-use of public data for individuals, businesses and the media. Its goal is not only to make public sector activities transparent, but also to encourage all other parties to make better use of this resource and so improve the performance in all sectors.[276]

No direct communication on political arguments, however the economic interest seems to be the leading drive also considering the importance of the financial sector in Luxembourg.

---

271 https://digital-luxembourg.public.lu/news/new-cybersecurity-strategy-luxembourg.
272 https://digital-luxembourg.public.lu/.
273 Trade & Investment Board Luxembourg, https://www.tradeandinvest.lu/news/becoming-a-leading-data-economy-2-2/.
274 https://securitymadein.lu/.
275 https://www.luxinnovation.lu/.
276 https://sip.gouvernement.lu/en/dossiers.gouvernement%2Ben%2Bdossiers%2B2018%2Bopen-data.html.

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors in general?

Luxembourg's government has decided not to influence the selection of software and hardware in general. It sees this guaranteed non-intrusion as the basis for further expansion of local companies, but also as a condition/necessity of the establishment of new companies with a particular focus on IT.[277]

Taking full advantage of this strategic location and of massive private and public sector investments, Luxembourg has become a key hub for ICT with highly secured data centers, connectivity & modern IT infrastructures, all of which are attracting more and more major international companies to set up their business in Luxembourg. The country boasts 23 high-tech data centers, the majority of which were built in the last 10 years, and high-speed international connectivity.

It has also been entrusted with storing data for NATO and the European Union – and now, the country of Estonia. In early June of 2019, Estonia transferred four core databases of information, including land and business registries, to servers at one of Luxembourg's high-security data centers. Six more transferred by September of the same year. It is believed to be the world's first "data embassy". These data centers hold cloud infrastructures and are supported by the Government. The Estonian data embassy will have the same protection and immunity as traditional embassies. This is a new concept in terms of international law and practice. The 'physical' embassies are sovereign territory under the Vienna Convention. This brings the same concept to the cyber world and data centres. This effectively means that officials from the host country will be barred from accessing the data. Furthermore, Google announced in 2019 its plan for a €1bn Data Centre in Bissen.[278]

Are there discussions specifically on 5G vendors?

Regarding security guidelines for 5G, a public consultation with all mobile market players was launched in March 2019, no final guidelines issued. Orange Luxembourg said that it is ready to launch 5G network in Luxembourg, after working with Ericsson to conduct 5G tests in lab conditions.[279]

Digital sovereignty with regard to skills, norms and educational aspects

Are there (educational) programs to raise awareness on digital sovereignty and the respective perception towards technology and data in the individual country?

No merely educational programs aimed at digital and technology skills such as the ones provided by the Luxembourg Tech School (LTS).[280]

---

277 https://www.solutions.lu/.
278 https://www.wort.lu/de/business/google-aeussert-sich-erstmals-zum-rechenzentrum-in-bissen-5dd69acada2cc1784e3503a9.
279 https://www.lteto5g.com/orange-luxembourg-ready-to-launch-5g/.
280 https://www.techschool.lu/.

Luxembourg has a state-owned infrastructure provider LuxConnect, a multi-tenant and multi-tier data center operator and dark fiber provider. The company acts as a facilitator and incubator in the ICT industry at local and international levels.

Are there (educational) programs to develop competencies, which promote DS?

No merely general educational programs like the national coalition for digital skills and jobs, launched on 29 May 2017 and Digital(4)Education. [281]

281 https://ec.europa.eu/digital-single-market/en/news/luxembourg-relaunches-its-digital-skills-and-jobs-coalition.

7.19 Digital sovereignty in Malta

Due to the country's size, Malta promotes itself as a "Test Bed" for ICT infrastructure projects. Although, there does not seem to be interest in the expansion of 5G. The public debate is rather dominated by health and security concerns.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

In the case of Malta, digital sovereignty is mainly defined by the National Cyber Security Strategy (NCSS). NCSS aims to strengthen the national cyber defence, to ensure the country's digital resilience to cyberattacks as well as the capability to protect its interests. Digital sovereignty in Malta can also be defined using a quote from the country's Cybersecurity Strategy: "*Malta has the right and obligation to defend its cyber-space territory to ensure that the security of the nation is maintained*."[282]

What is the approach towards DS?

For digital sovereignty specifically, no political arguments have been identified at all.

How is DS translated into concrete political and regulatory measures?

Not applicable

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors in general?

No specific selection criteria have been observed. Currently, most local ICT companies are software services and solution providers. There is limited foreign direct investment as well. Also, none of the mobile telephony operators have so far applied to introduce 5G technology. Instead of discussion on vendors, the debate in Malta seems to be more directed towards public health implications of 5G.[283]

Is there a discussion on other technology aspects with an impact on DS?

Malta aims to develop its expertise of Artificial Intelligence via its Strategy. It tries to generate investment and position the country as a hub for AI application. It is not clear yet in how far this contributes to Malta's sovereignty in the digital area.[284]

In addition, there is, since 2015, attention for the development of cloud computing capacities and usage in Malta by the Government. The Malta Cloud Forum (MCF) was set up in 2016 as a "*multi-stakeholder forum of parties interested in the cloud computing eco-system*", comprising companies, civil society, government and academia. It aims to

282 https://cybersecurity.gov.mt/strategy.
283 https://timesofmalta.com/articles/view/no-interest-so-far-to-introduce-5g-in-malta.773861.
284 https://malta.ai/wp-content/uploads/2019/11/Malta_The_Ultimate_AI_Launchpad_vFinal.pdf Executive Summary.

create an environment where cloud computing and related companies can flourish.[285] Again, it is not clear how yet how this has impacted Malta's sovereignty in crucial ICT areas.

Digital sovereignty with regard to skills, norms and educational aspects

Are there specific 'seals' which promote DS?

Our research did not identify any such measures.

Are there (educational) programs to develop competencies which promote DS?

No merely general education programmes aimed at boosting the development of ICT sectors in Malta. Examples are Digital Citizen (awareness programme which starts with the basic level of ICT competence[286]) and the Digital Malta National ICT Strategy 2020 (aimed to transform Malta into a regional hub for innovative start-ups in the areas of Blockchain, Artificial Intelligence, Internet of Things, Augmented Reality and others[287]).

Even the National Cyber Security Strategy emphasises the education and the awareness, regarding cyber security leading to national awareness campaigns.[288]

285 https://eurocloud.org/membership/associated/mca/.
286 https://digitalmalta.org.mt/en/Pages/Landing-Pages/DigitalCitizen.aspx.
287 https://mih.mt/.
288 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-malta.

7.20 Digital sovereignty in the Netherlands

The Netherlands are an important contributor for certification of and standards for ICT services and products through EU platforms with focus on DS. However, DS does not seem to be explicitly defined yet, hence the scope of DS is only medium.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

In 2018, the Dutch government (Ministry of Economic Affairs and Climate Issues) adopted the Dutch Digitalisation Strategy[289]. The focus is on capitalising on the economic and social opportunities associated with the digital transformation. However, the Dutch Cyber Security Agenda, third version (NCSA) links a strong cybersecurity with digital autonomy of governmental entities and companies by having own (security) solutions.[290]

The NCSA notes that "*Many Dutch organizations depend on a limited number of foreign providers of digital infrastructure services, as a result of which the impact in case of disruption is large.*"[291] Due to growing dependence on foreign suppliers of cybersecurity products and services and the increased demand for knowledge and capacities in this area, the different ministries coordinate with another.

What is the approach towards DS?

The Dutch Cyber Security Agenda furthermore notes that Cybersecurity is inseparably linked to national security as digitization has made national security concerns vulnerable to digital attacks. Hence, the NCSA is linked with the National Defence Strategy[292] and the 'Integrated Foreign- and Security Strategy' of the defence. Hence, the Netherlands advocate to strongly coordinate aspects of DS with the EU and NATO as "*The digital domain is not bound to borders.*"[293].

Furthermore, there is a focus on strengthening the quality of free software and the adoption of modern internet standards as this decreases risks.

In addition to the existing obligations for telecom providers in the Telecommunications Act, the proposed Cyber Security Act expands the number of vital providers that are subject to obligations. Sectoral regulators will monitor cybersecurity in sectors with vital infrastructure where this has not previously been the case.

---

289 Nederlandse Digitaliseringsstrategie https://www.rijksoverheid.nl/documenten/rapporten/2018/06/01/nederlandse-digitaliseringsstrategie.

290 Nederlandse Cybersecurity Agenda, https://www.ncsc.nl/onderwerpen/nederlandse-cyber-security-agenda/documenten/publicaties/2019/mei/01/nederlandse-cybersecurity-agenda.

291 NCSA, p.32.

292 Geïntegreerde Buitenland- en Veiligheidsstrategie en de Defensienota.

293 Nederlandse Cybersecurity Agenda, p.7, https://www.ncsc.nl/onderwerpen/nederlandse-cyber-security-agenda/documenten/publicaties/2019/mei/01/nederlandse-cybersecurity-agenda.

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors in general?

Part of the Cyber Security Agenda (NCSA) is a Roadmap for Digital Secure Hardware and Software (Roadmap DVHS), released in 2018 by the Ministries of Economic Affairs and Climate and Justice and Security. This Roadmap is 'work in progress' and aims to provide a coherent approach in promoting the digital security of hardware and software with public and private parties.[294]

There are no selection criteria yet for ICT vendors, but preparations are clearly on their way; the Roadmap DVHS of 2018 noted clearly that additional measures are required for the procurement of hard- and software, which impact the digital security[295]. The Netherlands are pushing at EU level for standard and certification of hard- and software which impact the digital security via the Cyber Security Act and a European Framework for certification of ICT services.[296]

There is also attention for the improvement of open source encryption, which decreases the safety risk and/or dependency on foreign encryption methods.

KPN, the leading mobile network operator, announced in April 2019 that it would select a Western supplier to build its core 5G mobile network, making it one of the first European operators to make clear it would not pick China's Huawei for such work[297]. However, in November 2019[298] it announced that it selected Huawei for the 5G Radio Access Network over the seemingly technically less ready competitor Ericsson. In February 2020, the Dutch Lower Chamber of Parliament adopted several motions from political parties coming from the 5G debate the week before. A majority of the Lower House asked the government to strictly assess the security of 5G networks, which should also include the Radio Access Network and other components.[299] In October 2020, KPN decided to use Ericsson for its 5G core network and not Huawei.[300]

Are there discussions on other technology aspects with an impact on DS?

The Netherlands is actively participating in a working group formed by the European Commission to develop a European cloud certification scheme. Cloud services are a central element of ICT products and services. Together with Germany and Austria, among others, the Netherlands has drawn up a recommendation for a European cloud certification scheme with a set of security requirements and the way in which an ICT supplier is accountable for these requirements.[301]

---

294 https://www.rijksoverheid.nl/documenten/rapporten/2018/04/02/roadmap-digitaal-veilige-hard-en-software.
295 Roadmap DVHS, paragraph 3.9.
296 NCSA, p. 15.
297 https://www.reuters.com/article/us-kpn-huawei-5g/dutch-telecom-kpn-wont-use-huawei-for-core-5g-network-idUSKCN1S20LQ.
298 https://www.lightreading.com/5g/ericsson-the-unready-loses-kpn-to-huawei/d/d-id/755883.
299 https://www.telecompaper.com/news/dutch-parliament-wants-strict-criteria-for-5g-safety--1326380.
300 Telecoms.com, 15 October 2020, see https://telecoms.com/506944/kpn-taps-ericsson-to-replace-huawei-in-5g-core/.
301 https://www.rijksoverheid.nl/documenten/kamerstukken/2019/06/20/kamerbrief-voortgang-roadmap-digitaal-veilige-hard-en-software.

Regarding an EU wide cloud (like GAIA-X) no formal decisions have been taken so far in the Netherlands. The initiative is being discussed and interested parties generally see the benefits of the initiative.[302]

In anticipation of the Cyber Security Agenda, the Netherlands has taken the initiative in a number of important areas to stimulate the application of international standards and to establish partnerships and frameworks, such as Partnering Trust, Secure Software Alliance and the Smart Industry Standardisation Platform.[303]

- *The Secure Software Alliance* aims to further develop 'secure software development' and ensure its quality. At its core, it's about making software products safe as early as possible by covering potential vulnerabilities at each stage of the product lifecycle. This is commissioned by the Ministry of Economic Affairs and the Ministry of Justice and Security via the Centre for Crime Prevention and Security (CCV).[304]
- *Partnering Trust;* In the context of the General Data Protection Regulation (*Algemene verordening gegevensbescherming - AVG* [305]) the Ministry of Economic Affairs, Agriculture and Innovation initiated the Partnering Trust project, which aims to standardise requirements for online ICT services in Europe.

Digital sovereignty with regard to skills, norms and educational aspects

Are there specific 'seals' which promote DS?

Not yet, but activities are on the way. The Netherlands pushes as well for mandatory certification or CE marking for all Internet-connected products. In addition, the Netherlands stimulates the application of international standards, partnerships and frameworks. The Netherlands connect proactively to relevant European and global standardization and certification initiatives via the NEN standardization platform. The Netherlands also engage in multilateral collaboration on Internet of Things standardisation, for example via the Global Forum on Cyber Expertise.[306]

Are there (educational) programs to develop competencies which promote DS?

Not directly focused at digital sovereignty. However, the NL does belong to the top EU countries in regards to digital skills/capacities; the university of Eindhoven and Delft have developed a significant tech campus and around Eindhoven a whole 'Brainport' has risen with the leading companies in ICT sector present.[307]

---

302 https://www.channelweb.nl/artikel/expertverslag/cloud-computing/6890493/5249091/iedereen-heeft-baat-bij-gaia-x.html ; https://www.technite.nl/gaia-x-of-de-kans-op-succes-voor-een-europese-cloud/.

303 https://www.rijksoverheid.nl/documenten/rapporten/2018/04/02/roadmap-digitaal-veilige-hard-en-software, p. 20 ff.

304 https://www.rijksoverheid.nl/documenten/kamerstukken/2019/06/20/kamerbrief-voortgang-roadmap-digitaal-veilige-hard-en-software.

305 Since 25 May 2018, the so called General Data Protection Regulation (*Algemene verordening gegevensbescherming - AVG*) applies. The AVG distinguishes between data controllers (those who collect personal data and determine the purposes and means of processing personal data) and processors (those who process personal data on behalf of the data controller). The AVG obliges both parties to enter into processing agreements in which the responsibilities and agreements between the parties are laid down. https://www.zeker-online.nl/partneringtrust/ and https://ecp.nl/project/partneringtrust/.

306 Nederlandse Cybersecurity Agenda, p. 28.

307 https://brainporteindhoven.com/int/.

7.21 Digital sovereignty in Poland

Poland incorporates DS especially in the field of cyber security but also in the field of open data. Together with the US, it also lobbies against using Huawei for the expansion of 5G.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

Focus on the cybersecurity dimension;

- On 31 October 2019, Poland's Ministry of Digitization has drafted a new cyber security strategy for 2019-2024. It will develop the country's National Cyber security System which allocated tasks and responsibilities to prevent and minimise the effects of cyber-attacks in Poland[308] as well as to improve data protection in the public, military and private sectors. It will also seek to expand Poland's information-exchange system and boost its cybersecurity technology potential.
- The previous Cyber Security Strategy (2017-2022) defined four objectives, such as to ensure a coordinated capacity to combat cyber-threats at national level, to increase Poland's capability to counter such threats, to enhance the digital competences of local entities and to strengthen Poland's international position in the field of cyber security. This is done through NASK, the national research institute supervised by the Ministry of Digital Affairs, whose tasks "*range from responding to cyber security threats in the network at the operational level […] to educational and R&D tasks in the field of security, reliability and efficiency of ICT networks*". [309]
- Furthermore, the Ministry of National Defence plays a central role to ensure the cyber resilience of Poland. In 2019, the Ministry presented the concept of a cyberspace defence command and a set of activities related to the development of cybersecurity capacities.[310]

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors in general?

There is no a specific selection criteria system yet but the Government's priority in this regard will be to create a national evaluation system, which aims to increase trust in the used hardware, software and cryptography. Poland actively participates in the establishment of a European system for evaluation and certification of products and

308 https://www.thefirstnews.com/article/cybersecurity-forum-opens-in-katowice-south-poland-8379.
309 https://ccdcoe.org/uploads/2018/10/NCSO_Poland_2017.pdf.
310 https://www.gov.pl/web/national-defence/the-national-defence-ministry-creates-the-cyberspace-defence-forces.

services in the IT and communications sector. Examples are the SOG-IS MRA and the CCRA.

Regarding the security aspect of 5G networks, the following development is observed:

- In December 2019, in the context of 5G security; Digital Minister Marek Zagórski noted during an interview that "*Poland will introduce tougher controls that would "limit the use of [telecom equipment] vendors who are suspicious or who are not necessarily trustworthy, or who do not stick to the security standards*,".[311] However, he also noted that "*Security of end devices is something different than security of the core of the network*", while explaining that different parts of the system could have different security requirements. [312] The Polish telecommunications infrastructure has been heavily reliant on Chinese provider Huawei, with the company's equipment previously used by Polish operators in 5G trials.
- In July 2019, Huawei announced plans to invest three billion zloty (670 million euros) in Poland over the next five years, however, this investment may be reduced if Huawei does not play a part in developing the country's 5G network.[313]
- In September 2019, "*Prime Minister Mateusz Morawiecki signed a joint declaration with US Vice President Mike Pence on protecting 5G networks from untrustworthy suppliers, including an evaluation of whether they are controlled by foreign governments.*"[314]
- In May 2020, "*a Polish government minister told Reuters that it was unlikely that Poland could exclude all Huawei equipment from its next generation mobile networks, and instead would focus on improving security. Karol Okoński, a former deputy digital affairs minister in charge of cyber security, said the country would be unable to finance the replacement of Huawei equipment by telecoms operators, but could look into imposing further restrictions around 5G networks*."[315]

Is there a discussion on other technology aspects with an impact on DS?

Data is an essential enabler for the development of AI solutions. For this reason Poland has a strong focus on supporting the availability of data and related data analysis. Its strategy foresees to further extend the open data platform containing open data collections of the public administration, creating virtual data warehouses for companies to share their industrial data in trustworthy and cyber secured data spaces.

311 https://www.telecomlead.com/5g/poland-may-impose-stricter-security-demands-for-5g-network-93483.
312 https://www.reuters.com/article/us-poland-5g/poland-may-vary-security-demands-for-different-parts-of-5g-minister-idUSKBN1YM1V7.
313 https://notesfrompoland.com/2020/05/12/first-commercial-5g-network-launched-in-poland/.
314 https://notesfrompoland.com/2020/05/12/first-commercial-5g-network-launched-in-poland/.
315 https://notesfrompoland.com/2020/05/12/first-commercial-5g-network-launched-in-poland/.

To facilitate data analyses, the Polish government intends to invest in cutting-edge digital and telecommunication infrastructure, such as HCP centres and increased connectivity through 5G networks.

Another focus is on building its competencies in the cloud computing sector; there is a partnership between PKO Bank Polski along with the Polish Development Fund, which is called Domestic Cloud Provider in cooperation with Google. According to Google Cloud CEO Thomas Kurian, the goal is "*to accelerate cloud adoption by large and small businesses alike, across all industries*," and to *"help Polish businesses on board to the cloud."* **316**

Digital sovereignty with regard to skills, norms and educational aspects

Are there norms or state 'seals of approval' promoting DS?

Our research did not identify any such measures. PCA is the national accreditation body for Poland, responsible for assessing the competence and capability of organisations that provide certification, testing, inspection and calibration services. **317**.

Are there (educational) programs to develop competencies, which promote DS?

To support the re-use of data in Poland, there are several programs to train and educate persons and companies; starting with the 'Open Data Programme' in 2016, data became available via one website. In 2017, there was a significant increase in the number of information resources accessible via this Central Repository of Public Information. In 2018, the Polish Ministry of Digital Affairs published guidelines to prepare and share data for re-use including certain Application Programming Interface (API) Standards. Aim was to ensure a higher quality of data by the public administration. Open data may now be reused for research or business purposes.

In addition, there are the general digitalisation programs like 'The Future Industry Platform'**318** and the Programme for a Digital Poland (OPDP)2, introduced in 2014 for 2014-2020, which is designed to consolidate the digital foundations of the country's development.

The Polish Government introduced the Morawiecki Plan, which provides industrial financing over a 25-year period, and pursues an agenda of reindustrialization through new partnerships, export-oriented support measures and comprehensive regional development.

316 https://data-economy.com/google-cloud-partners-with-dcp-with-new-cloud-region-in-poland-underway/.
317 https://www.cybersecurityintelligence.com/polish-centre-for-accreditation-pca-5509.html.
318 Announced as part of the Responsible Development Plan ('Morawiecki Plan') by the Ministry of Finance and Development in 2016. See https://ec.europa.eu/growth/tools-databases/dem/monitor/content/poland-%E2%80%9Cinitiative-polish-industry-40-%E2%80%93-future-industry-platform%E2%80%9D.

7.22 Digital sovereignty in Portugal

Portugal has a strong focus on network integrity and the defence of cyber-attacks. Portugal described digital resilience as a national task. Its DS scope can be described as medium.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

DS is on the agenda and very much aligned with EU policies. In 2015, the Council of Ministers in Portugal approved the first National Strategy for Cyberspace Security (NSCS), with the aim of creating a safe and efficient cyberspace for all[319]. In 2017, the National Cybersecurity Council was created and tasked with the update of the NSCS. In 2018, the legal framework for cybersecurity was established and the Superior Council for Cyberspace Security was founded to support the Prime Minister on cyberspace security issues.[320]

In 2019, the renewed strategy was issued as a "*structuring instrument for national capacity building in this area, defining the framework, the objectives, and the lines of action of the State on the security of cyberspace, in accordance with the national interest*." This strategy has 3 strategic objectives: 1) maximizing resilience, 2) promoting innovation and 3) generating and securing resources. The National Cybersecurity Centre (CNCS) is the authority, which coordinates the implementation of the NSCS and the monitoring thereof.[321]

Furthermore, the cyber security strategy notes that "*considering that much of the technological infrastructure that makes up the cyberspace is owned by private sector entities, the role of the Portuguese state is to guard that cyberspace is used in a responsible manner*." And that "*due to the interdependence of technological infrastructures, it has the duty to reinforce cooperation between national structures to maximize digital protection and the digital resilience of Portugal.*"

What is the approach towards DS?

The focus in Portugal is to prevent network integrity breaches and building skillsets for digitization. Criminal intent is tackled by multiple initiatives of the armed forces and coordinated response teams. Regulation issued by Anacom focuses as well on network integrity.

The cyber security strategy identifies threats from 2 categories: state agents and non-state agents. The first category stems from actors with a political, military and economic motivation, who might target critical infrastructures and disrupt essential services which support a proper functioning of society. The second category are actors with pecuniary motives, although there are also politically and ideologically motivated actions, aimed to denigrate institutional images and diminish the reputation of targets.

319 The Resolution of the Council of Ministers No. 36/2015, 12 June 2015.
320 Law 46/2018 of 13 August 2018 transposing EU Directive 2016/1148.
321 Resolution of the Council of Ministers No. 92/2019.

The Council of Ministers of Portugal adopted multiple decisions in 2019, among them a decision to found a working group on 5G and cyber security.[322] National telecom regulator, Anacom, coordinates this working group together with representatives from the CNCS and Government entities. One of the goals is to do a national assessment of cybersecurity risks affecting 5G networks, as well as participating in a periodic review at European level. No output yet published from this.

Anacom also issued begin 2019 a law regarding space activities, which, among others, guards Portugal's sovereignty described as "*Protecting the political and strategic interests of the Portuguese Republic, ensuring that private space activities are not contrary to them.*"[323]

In April 2019, Anacom also issued Regulation on the security and integrity of electronic communications networks and services. The focus of this regulation is on network integrity and prevention of security breaches and emergency situations. [324]

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors?

The Portuguese government undertook a national risk assessment regarding the security of 5G networks. Based on this assessment, a set of common measures was identified, to be implemented to mitigate the detected security risks (not published). [325]

Regulator Anacom does not exclude any provider for the delivery of 5G technology. There is an ongoing workgroup which evaluates and classifies the telecommunications suppliers that exist in the Portuguese market in profiles, according EU criteria. Only if a supplier is classified as "high risk" should "a set of restrictions" be observed.[326]

Furthermore, the Council of the Ministers issued a resolution in 2020, on the strategy and timing of 5G networks. It notes that, considering the security requirements, a national risk assessment has to be carried out by the Cyber Security Council to monitor the 5G networks.[327]

However, no specific guidelines toward 5G vendors has been found and despite repetitive pressure from the US, Portugal remained steadfast in its decision to retain limited use of Huawei technology in the developing 5G rollout.[328]

---

322 Under the terms of Article 199 (g) of the Constitution, see decision 8, https://www.anacom.pt/render.jsp?contentId=1507487.

323 Decree-Law no. 16/2019, of 22 January 2019, article 1d), see https://www.anacom.pt/render.jsp?contentId=1475024.

324 Regulation No. 303/2019, 1 April 2019, https://www.anacom.pt/streaming/Regulation303_2019SecurityIntegrityCom_rev.pdf?contentId=1475003&field=ATTACHED_FILE.

325 Following EU Commission Recommendation No. 534/2019, of 26 March 2019 on the cybersecurity of 5G networks.

326 See https://jornaleconomico.sapo.pt/en/news/huawei-anacom-says-no-one-is-excluded-from-5g-in-portugal-546081.

327 Resolution of the Council of Ministers No. 7-A 2020, of 7 February 2020

328 Portugal Resident, 19 February 2020, https://www.portugalresident.com/new-us-bid-to-twist-portugals-arm-over-5g-development-with-huawei/.

Are there discussions on other technology aspects with an impact on DS?

There is a national strategy on Artificial Intelligence (AI), which was launched in October 2018 within the scope of the nationwide INC0DE.2030 program. However, the focus is more on stimulating innovation, testing facilities, knowledge transfer and retaining talent in relation to AI. No specific mention of digital resilience here.[329]

No information found on data / cloud sovereignty or certification efforts.

Digital sovereignty with regard to skills, norms and educational aspects

Are there 'seals' which promote DS?

Our research did not identify any such measures. Focus is on providing information to gain trust from the general public regarding the use of (government) digital platforms.

Are there (educational) programs to increase competencies which promote DS?

Promotion of digital skills is geared towards increasing the (business) position of Portugal, less focus on decreasing the dependence in crucial areas. This is also reflected in the latest national cyber security strategy; one of the objectives is to "*Promote Innovation: Foster and enhance national innovation capacity by affirming the cyberspace as a domain for the economic, social and cultural development and prosperity".*

There are so called Fablabs and innovation hubs for different sectors, which develop 'Industry 4.0' capacity and digitization in general. There is a Digital Innovation Hub focusing on manufacturing, one targeting the health sector and one specialised in the agricultural sector.

329 AI Portugal 2030 Strategy.

7.23 Digital sovereignty in Romania

Although Romania is lacking behind digitalization in general, it has close ties to the US as large US technology firms are investing in local data centres. Romania has also partnered up with the US for its cyber security strategy and for the roll out approach of 5G.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

Romania does not define digital sovereignty explicitly in their National Strategy for the Digital Agenda for Romania – 2020. The strategy covers digitalisation more generally: e-Government, Interoperability, Cyber Security, Cloud Computing and Social Media; ICT in education, culture and health; ICT in e-commerce, and research, development and innovation in ICT; and Broadband and digital infrastructure services. This strategy was published in 2015 and developed by the Ministry for Information Society.[330]

What is the approach towards DS?

No direct approach towards DS.

> The National Strategy on Digital Agenda for Romania targets directly the ICT sector and aims to contribute to economic growth and increase competitiveness. It hopes to achieve both by direct action and support of the development of effective Romanian ICT and through indirect actions such as increasing efficiency and reducing public sector costs in Romania, improving private sector productivity by reducing administrative barriers in relation to the state, improving the competitiveness of the labour force in Romania and beyond.[331]

Besides working with the EU, Romania collaborates closely with the USA on cybersecurity and digital infrastructure. Romania's Minister of Information Society also points out that cybersecurity and trust in public services are a national priority with the Romanian Government, while Romania is advocating the adoption of a new legislative package regarding personal data protection. Furthermore, in August 2019, ambassadors from Romania and the United States signed a memorandum for the development of secure 5G networks, including criteria for selecting companies permitted involvement in 5G infrastructure.

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors in general?

> In December 2019, the National Authority for Administration and Regulation in Communications (ANCOM) launched public consultations for its 2020 action plan, which has a focus to complete the tender for granting rights to use the frequency

330 https://www.gov.ro/en/government/cabinet-meeting/national-strategy-on-the-digital-agenda-for-romania-2020.

331 https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Romania_2019.pdf.

> bands for the provision of 5G communications in early 2020. […]
> The Romanian President recently noted that no state policy has yet been agreed with respect to 5G implementation.[332]

For 5G, in August 2019, ambassadors from Romania and the United States signed a memorandum for the development of secure 5G networks, including criteria for selecting companies permitted involvement in 5G infrastructure[333]. According to the Romanian Presidency, the memorandum of understanding "*does not refer to a particular company but clarifies certain criteria relating to transparency and its compatibility with the rule of law"*[334]. It focuses on a careful and complete evaluation of 5G vendors as part of a risk-based approach, defining the following vendors' evaluation criteria:[335]

- Whether the vendor is subject, without independent judicial review, to control by a foreign government;
- Whether the vendor has a transparent ownership structure, and
- Whether the vendor has a history of ethical corporate behaviour and is subject to a legal regime that enforces transparent corporate practices.

Is there a discussion on other technology aspects with an impact on DS?

Romanian relevant authorities focus on developing a "*G-Cloud (Governmental Cloud), a private or community cloud especially designed for national governmental use. The Governmental Cloud has a double role. The first issue refers to the relation of governments with citizens in the eGovernment context."* However, "*there is also a secondary issue, equally important, related to determining a technical work frame for the interoperability of governmental organizations.*"[336]

Digital sovereignty with regard to skills, norms and educational aspects

Are there specific 'seals' which promote DS?

SRAC CERT is the Romanian certification body with the largest recognition of the marks and certificates nationwide due to IQNet Partnership and RENAR accreditation body - signatory of EA-MLA (European Multilateral Agreement). The only relevant standard / certification offered by SRAC and other relevant bodies is the ISO/IEC 27001:2018, which is based on the implementation of security policies, procedures and methods, aimed at protecting the organization information and assets.[337]

---

332 https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g/romania.
333 https://en.euractiv.eu/wp-content/uploads/sites/2/special-report/EURACTIV-Event-Report-Striking-a-balance-IT-infrastructure-and-digital-sovereignty.pdf.
334 https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g/romania.
335 https://media.hotnews.ro/media_server1/document-2019-11-3-23464357-0-memorandum-5g-romania-sua.pdf.
336 https://www.trusted.ro/wp-content/uploads/2014/09/Digital-Agenda-Strategy-for-Romania-8-september-2014.pdf.
337 https://www.srac.ro/en/information-security-isoiec-27001.

Are there (educational) programs to develop competencies, which can improve DS?

Not directly, more general ICT supporting programs:

- Romania has committed to invest in digital technologies, via EU-coordinated programmes. One of the measures to support SMEs is the “Start-up nation” programme. About 10,000 companies per year are targeted, with a maximum financing of EUR 44,000 that can be obtained for e.g.: IT equipment, website, software licenses, courses, consulting etc. (not all related to IT). In 2017, over 8,000 new companies were created that signed financing programmes, in a total amount of RON 1.7 billion (about EUR 380 million).[338]
- Moreover, there are five (5) fully operational Digital Innovation Hubs in Romania offering: Ecosystem building services, scouting, brokerage, networking, incubator / accelerator support and access to funding and investor readiness services.[339]

338 https://start-upnation.ro/.
339 https://s3platform.jrc.ec.europa.eu/digital-innovation-hubs-tool?p_p_id=digitalinnovationhub_WAR_digitalinnovationhubportlet&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&formDate=1589725153839&freeSearch=&countries=22&evolStages=3&servicesProvided=2&servicesProvided=10&servicesProvided=13&h2020=false.

7.24 Digital sovereignty in Slovakia

Slovakia's only concern regarding DS is cyber security hence its general scope of DS is narrow. The country is working on a government cloud. No restriction for 5G vendors has been made public.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

Only cybersecurity aspects to be found, no direct link to digital sovereignty.

In 2015, Slovakia published the national cyber security strategy – the "Cyber Security Concept of the Slovak Republic for 2015-2020" – with an accompanying "Action Plan for the Implementation of the Cyber Security Concept of the Slovak Republic for 2015-2020."[340] It defines the starting position and the goals of the Slovak Republic in the field of cyber security. The strategic goal of cyber security in the Slovak Republic is to achieve an open, secure, and protected national cyber space especially by building trust in the reliability and security of, above all, critical information and communication infrastructure, as well as building certainty that this will perform its functions and serve national interests also in cases of cyber-attacks.

What is the approach towards DS?

Digital sovereignty in Slovakia incorporates two main aspects: cyber security and information security, which includes personal data protection as well. The common strategic goal is to "*establish an open, secure, and protected national cyberspace*."[341]

One of the most serious problems in the area of cyber security in the Slovak Republic is the fact that the protection of cyber space is not yet explicitly and integrally regulated in valid law. "*Existing capacities and mechanisms in the area of network and information security are no longer sufficient to keep the pace with a dynamically changing environment of threats and to provide a sufficiently high and, above all, legally effective, level of protection in all areas of the state's administration and of social life*."[342]

The National Security Authority (Národný Bezpečnostný Urad - NBU)[343] is the central government body in Slovakia for the Protection of Classified Information, Cryptographic Services, Trust Services and Cyber Security. The NBU operates the national Computer Emergency Response Team (SK-CERT) and acts as a national point of contact for cyber security in relation to the European Union. It also participates in international exercises such as Cyber Coalition, annually organised by the NATO, and acts as a co-organizer of that exercise in conditions of Slovakia.[344]

---

340 https://potomacinstitute.org/images/CRI/CRI_Slovakia_Profile-Digital.pdf.
341 https://www.nbu.gov.sk/wp-content/uploads/cyber-security/Cyber-Security-Concept-of-the-Slovak-Republic-for-2015-2020.pdf.
342 https://www.nbu.gov.sk/wp-content/uploads/cyber-security/Cyber-Security-Concept-of-the-Slovak-Republic-for-2015-2020.pdf.
343 https://www.nbu.gov.sk/en/index.html.
344 https://www.sk-cert.sk/.

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware vendors in general?

Four Slovak mobile operators decide on suppliers for future 5G networks. The only operator who has it clear already is Orange. It announced cooperation with Nokia, reported Zive.sk. Slovak Telekom has not taken any decision yet. O2 Slovakia runs a tender to select a supplier. Finally, the fourth MNO 4ka admits being in touch with four suppliers: ZTE, Nokia, Huawei and Ericsson.

Is there a discussion on other technology aspects with an impact on DS?

In October 2019, the Slovakian government published the Action plan for the digital transformation of Slovakia for 2019 –2022 focusing on creating a legislative and regulatory framework for AI. Among others it will assess to what extent the current AI regulation models on data management, cyber security and intellectual property should be revised.

Furthermore, a coordinated Data Center of Municipalities (DCOM). It provides citizens and municipalities solutions in the form of "Software as a Service" ("SaaS"), which enables employees of the authorities to use software applications. [345]

Digital sovereignty with regard to skills, norms and educational aspects

Are the specific 'seals' which promote DS?

Our research did not identify any such measures.

Are there (educational) programs to develop competencies, which promote DS?

No, only specific training related to cyber security supported by the Action Plan and also the National Strategy for Information Security in the Slovak Republic 2009-2013:

- professional training on information assurance of specialists and decision makers (managers) from the public administration (since 2013) – it´s aim was to contribute to enhancing of awareness and competence in the field of information assurance;
- including information security in IT or other classes taught at secondary schools;
- publishing specialised literature and methodology documents addressing particular issues of information security.

Another project is TECHNICOM, a university science park for innovative applications with the support of knowledge technologies. The aim of the project is to create an environment for top applied research and development, which will be directly supported by an efficient system of acceleration of high-tech business based on the spin-off and start-up principles of transfer of knowledge gained in research into commercial and public practice.[346]

345 https://www.dcom.sk/.
346 https://www.upjs.sk/en/faculty-of-science/technicom/.

National Centre of Robotics is an association established under the patronage of faculty of electrical engineering and information technology, Slovak technical university in Bratislava.[347]

347 https://nacero.sk/language/en/.

7.25 Digital sovereignty in Slovenia

Slovenia does not have DS on the agenda and is more focused on digitalization itself and the development of the ICT sector. Besides, Slovenia puts effort into the development of AI and a government cloud.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

Not really. Mostly focus on cybersecurity; the objectives are ensuring safe operation and availability of key ICT systems in the event of major natural and other disasters.[348]

What is the approach towards DS?

Since 2016, the Government of the Republic of Slovenia adopted a long-term strategy on the development of the information society. The detailed objectives of this strategy included secure cyberspace and raising general awareness of the importance of ICT technologies for the development of society. The Strategy's vision addresses that "*at the same time, a high level of protection of personal data and communication privacy in a digital society should be ensured. This [shall] create trust and confidence in digitalization and cyberspace.*"[349]

Among the implemented measures is the establishment of a vendor management team and a Government Cloud (DRO). In 2015, the on premise Government Cloud was established and consequently public administration IT systems were migrated to this cloud infrastructure and its data centres.[350]

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware vendors in general?

Slovenia has started several discussions regarding 5G vendors, while the US urged Slovenia to apply a 'trusted vendor' strategy for 5G.

> […] Robert Strayer, the deputy assistant secretary for cyber and international communications and information policy, noted the importance of adopting appropriate security measures in order to protect sensitive data. He said that the company that provides the fifth generation wireless technology must be resident in an environment where there is rule of law, due process and independent judiciary.

---

348 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Slovenia_2016_Cyber_Security_Strategy.pdf.

349 https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Slovenia_2019_0.pdf.

350 https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Slovenia_2019_0.pdf.

Regarding which provider of 5G Slovenia should choose,

> Strayer said that the US wanted Slovenia to make its own decision about which kind of providers it wants to have. However, he said it was important that it 'adopt a set of security standards that include looking at the laws that are in place where the companies are headquartered'.[351]

Is there a discussion on other technology aspects with an impact on DS?

The development of a national AI strategy for Slovenia is high on the agenda; a high-level working group consisting of representatives of various ministries, research institutions and government departments has been put in place to develop actions and policies in AI. [352]

Digital sovereignty with regard to skills, norms and educational aspects

Are there specific 'seals' which promote DS?

Our research did not identify any such measures.

Are there (educational) programs to develop competencies, which promote DS?

No, merely educational programs to raise awareness on using the internet in a safe manner and start up platforms to support companies. [353]

351 http://www.sloveniatimes.com/us-urges-slovenia-pick-trusted-vendors-of-5g.
352 https://ec.europa.eu/knowledge4policy/ai-watch/slovenia-ai-strategy-report_en.
353 https://www.betterinternetforkids.eu/web/slovenia/profile and https://www.startup.si/en-us/about-us.

7.26 Digital sovereignty in Spain

In Spain, attributes of DS can only be found in its cyber security strategies. DS itself is not explicitly defined and in the media, DS is only discussed in the context of EU initiatives.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

Not directly, we have observed only a cybersecurity strategy and the general digitalisation plans. The Digital Agenda for Spain was launched in 2013 as the Government's strategy to develop the digital economy and society in the country. This strategy was configured as the umbrella for all Government's actions in the area of Telecommunications and the Information Society.[354] In the same year, also the National Cybersecurity Strategy was adopted and reviewed in 2019.[355]

What is the approach towards DS?

The recently reviewed National Cybersecurity Strategy 2019 points to a sovereign approach for Spain. It consists of primarily strategic decisions. As far as concrete technological measures are concerned, there is currently a debate on what measures must/should be taken with regard to 5G.

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors in general?

The Secretariat of State for Digital Advancement (SEAD) performed a public consultation from November to December 2019 in relation to the development of security standards for 5G networks and services. The aim was that any person or entity can make contributions in relation to this standard.[356] No results have been published so far though.

Of interest may be that the Spanish telecom giant Telefonica has awarded part of the contract to deploy its 5G core network to Chinese vendor Huawei.[357]

Are there discussions on other technology aspects with an impact on DS?

Back in 2013 the Public Administration had already begun the development of a cloud service, taking its own technological infrastructure, the SARA network, as a starting point. On January 15, 2013, the Superior Council of Electronic Administration chaired by the Minister of Finance and Public Administration, declared SARA a project of priority

354 https://avancedigital.gob.es/planes-TIC/agenda-digital/Paginas/agenda-digital-para-Espana.aspx.
355 https://www.dsn.gob.es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional and https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019.
356 https://amiitel.org/consulta-publica-previa-a-la-elaboracion-de-una-norma-sobre-seguridad-de-las-redes-y-servicios-5g/.
357 https://www.rcrwireless.com/20191209/5g/telefonica-spain-selects-huawei-part-5g-core-network-report.

based on which a Spanish Public Administration's private cloud should be build.[358] This was again mentioned in the strategy paper 'Plan de Transformacion Digital de la Administracion 2015-2020' mentioning that infrastructures and technological platforms should be consolidated by setting up a hybrid cloud (SARA cloud) offering software, platform and infrastructure as a service (Saas, Paas and Iaas).[359]

AENOR (Asociación Española de Normalización y Certificación) designed the Cybersecurity and Privacy Ecosystem for the new digital era, based on ISO international standards/standards, as well as current Spanish and European laws and regulations. AENOR certifications of Information Security Management System ISO/IEC 27001 and the National Security Scheme (ENS) have been combined for organizations to have a better management of cyber security, focusing on the continuous improvement of risk and threat control.[360]

Digital sovereignty with regard to skills, norms and educational aspects

Are there specific 'seals' which promote DS?

AENOR (Asociación Española de Normalización y Certificación) certifies entities and systems according Information Security Management System ISO/IEC 27001 and the National Security Scheme (ENS). Aim is to have a better management of cyber security, focusing on the continuous improvement of risk and threat control.[361]

Are there (educational) programs to raise competencies, which promote DS?

Overall, Spanish enterprises are well positioned in terms of digital transformation. No specific information regarding the use of EU or Non-EU providers of software/hardware.

358 http://www.preparatic.org/tag/informacion-nube-sara/.
359 https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Estrategia-TIC-AGE.html.
360 https://revista.aenor.com/348/isoiec-27001-y-ens-binomio-perfecto-para-la-ciberseguridad.html.
361 https://revista.aenor.com/348/isoiec-27001-y-ens-binomio-perfecto-para-la-ciberseguridad.html.

7.27 Digital sovereignty in Sweden

Sweden has a strong focus on data sovereignty and open government data. It raised concerns that public/private data is stored in foreign data centres or in local data centres provided by foreign companies.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

Sweden's focus is on building an open, data based, society which enhances its capability to use and enhance development in different sectors and for example AI.

The actions of the Swedish government are towards strengthening the digital autonomy of the country. Even if it is not clearly stated within the government agenda, these actions show that Sweden is willing to act as a leading country in this area.

In June 2017 the government presented Sweden's first National Cyber Security Strategy. The strategy was then supplemented with an appendix in July 2018, which, among other things, included an overview of ongoing and completed measures initiated by the government 2017-2018.

At the beginning of March 2019, seven government agencies with responsibilities in the field of cyber security also presented a joint action plan to implement the strategy at the agency level.

What is the approach towards DS?

Sweden faces the issue that a large number of authorises, including authorities on municipality and regional level are already using many different cloud services - for personal data and / or data that is confidential. These providers are coming from different countries where their governments have the right to access and control this data. Hence, the question is raised whether it is appropriate that a Swedish authority entrust parts of its community-carrying activities to a service provider that is under the jurisdiction of another state with the possibility for that state to access information within the activity without Swedish consent.[362] The political arguments conclude on the idea that Sweden needs to formulate a clear authority-shared strategy and a long-term plan of action on the control of data.

How is DS translated into practical measures?

When the government publishes open calls for stakeholders or potential vendors it seems that the government strategically prefers alliances that are state owned or that their base and activity are covered by the Swedish law.[363] The main challenge in the next few years, in respect of cloud computing services, is to ensure compliance under

362 Sweden's digital sovereignty is threatened by IT services in the cloud https://aigine.se/files/_Sweden's%20digital%20sovereignty%20is%20threatened%20by%20IT%20services%20in%20the%20cloud_%20-%20DN.SE.pdf.

363 This is not according to some regulation and only a perception that comes out from the government's actions.

the GDPR while using and providing cloud computing services. Notably, many cloud suppliers have been swift to ensure that their contracts comply with the requirements under the GDPR for data-processing agreements.

In this context, the Swedish Post and Telecom Authority (PTS)[364] plays a major role. PTS is one of the supervisory authorities for the NIS Directive in Sweden. They are responsible for the supervision of essential services within the digital infrastructure and for digital services. Their supervision involves monitoring the companies' compliance with the law and with the Swedish Civil Contingencies Agency's regulations. The primary aim is to assess whether the providers meet the requirements for security measures and incident reporting.

Digital sovereignty and technological aspects (hardware & software)

Are there selection criteria for hardware / software vendors?

Companies that supply certain types of (digital) crucial infrastructure and certain digital services are subject to information security requirements following the transposition of the NIS Directive in Swedish law on 1 August 2018. In accordance with the regulations, these companies are to work with information security systematically and are to report any incidents to the Swedish Civil Contingencies Agency (MSB).[365]

Services subject to the NIS Directive are categorized as essential services or digital services. Several sectors are supplying essential services, such as energy, transport as well as health and medical care. The sector that PTS supervises is digital infrastructure. In October 2019, PTS held a consultation on how to enhance security of networks and services, which contained among others, a risk assessment prior to procurement and documentation of contractors and their assignments of ICT.[366]

There have been discussions on criteria for 5G vendors, in the context of the obliged national risk assessment of 5G networks. Huawei is not restricted in Sweden although there is positive sentiment towards national supplier Ericsson which is one of the largest employers in Sweden and enduring strong competition from Huawei worldwide.

The Swedish Post and Telecoms Authority said early 2020 that there would be no unilateral ban on Huawei. However, all vendors who want to participate in the Nordic country's 5G networks must submit to an independent security review by the country's Armed Forces and Security Services.[367]

End October 2020, PTS announced that it barred Huawei and ZTE from supplying the winners of the coming 5G spectrum auction. Furthermore, that licence winners reusing already installed equipment from Huawei and ZTE, would need top phase out this equipment by 1 January 2025 at the latest. The exclusion is not only for the core network, but also for the radio access network, transmission as well as service and maintenance work. Stated reason was national security concerns following

364 https://www.pts.se/en/.
365 https://www.pts.se/en/english-b/internet/information-security-for-essential-services-and-digital-services/.
366 https://pts.se/en/news/telefoni/2019/regulatory-amendments-to-enhance-security-of-networks-and-services/.
367 https://www.chinadaily.com.cn/a/202002/11/WS5e41e5bfa31012821727674b.html.

assessments by the Swedish Armed Forces and the Swedish Security Service, as required by new rules enacted at the start of 2020.[368]

Are there discussions on other technology aspects with an impact on DS?

No other information found**.**

Digital sovereignty with regard to skills, norms and educational aspects

Are there (educational) programs to increase competencies, which promote DS?

Our research did not identify any such measures. However in general, a strong focus on on digital skills is observed. The Swedish government decided to strengthen the national curriculum in regards to digital skills.[369] As from July 1st 2018, digital skills are an essential part of the Sweden national curriculum in compulsory and upper secondary schools. With this decision the government aims at strengthening the digital knowledge of students and teachers.

In Sweden there are many acceleration programs and start-up hubs supporting the tech community on a daily basis. The start-up ecosystem of Sweden seems to be one of the most promising compared to other EU countries.[370]

368 Telecoms-com, 20 October 2020, see https://telecoms.com/507001/sweden-bans-huawei-and-zte-from-its-5g-networks/.
369 https://eacea.ec.europa.eu/national-policies/eurydice/content/digital-skills-enter-sweden-schools_en.
370 https://www.eu-startups.com/2019/01/stockholms-startup-ecosystem-at-a-glance/.

7.28 Digital sovereignty in the United Kingdom

Concerning DS, the UK is also mostly concerned with its cyber security. Although the UK states explicitly that in cyberspace, sovereignty must be defended, the country is mostly concerned about state funded hacking. The UK has the most restrictive approach for its 5G expansion and has excluded Chinese vendors for this task. For data storage, the UK also seems to want to reduce dependency from US firms.

Digital sovereignty in general

Is digital sovereignty (DS) on the agenda of the government?

As the UK left the EU on 31 January 2020 and negotiations with the EU about the future relationship are still ongoing, the UK definition of "sovereignty" seems to be very much in contrast to the EU's definition. Although concrete strategies are still in the work, written statements from the parliament indicate this trend: The UK will in future "*develop separate and independent policies*" in numerous areas, which also includes "*data protection*"[371]. Whether EU member states will have different agreements on data transfer and trade in general with the UK than the US or China is difficult to foresee.

In UK's digital strategy, which was published March 2017 by the Department of Digital, Culture, Media & Sports, digital sovereignty is not picked out as a central theme and is not mentioned.

Furthermore, digital sovereignty is also not explicitly mentioned in the "National Cyber Security Strategy 2016 to 2021" published in 2016 by the Cabinet Office and HM Treasury, however, "sovereignty" in general. In the context of cyberspace, the strategy states that to disrupt cyber threats, which include threats to the infrastructure, "*world-class sovereign capabilities*" are required. The strategy explicitly states that in the cyberspace, interests and sovereignty must also be defended.[372]

In the context of data storage outside Europe (and inside the United States), the UK government concludes in a Joint Committee on the National Security Strategy, that *"[t]he cornerstones of UK national security are being undermined […] [by, among others] the growing strains on the UK's relationship with the United States*"[373].

What is the approach towards DS?

The "National Cyber Security Strategy 2016 to 2021", which is more a strategy for cyber security and state sovereignty than digital sovereignty per se, two strategies to secure sovereignty are mentioned: Offensive cyber capabilities, which involve direct attacks to "*opponents' systems or networks, with the intention of causing damage, disruption or*

371 UK Parliament (2020): UK / EU relations: Written statement - HCWS86, retrieved from: https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2020-02-03/HCWS86/.

372 HM Government (2016): National cyber security strategy 2016-2021, p. 47.

373 Revisiting the UK's national security strategy: The National Security Capability Review and the Modernising Defence Programme, page 32.

destruction" and cryptography to protect sensitive information. For cryptography, the object is to keep political control over cryptographic capabilities to "*protect UK secrets*"[374].

The objectives for offensive cyber security, as stated in the "National Cyber Security Strategy 2016 to 2021" are deterrence and operational purposes.

Furthermore, as stated in the "UK telecoms supply chain review report" (2019)[375] by the Secretary of State for Digital, Culture, Media and Sport, a wide-ranging valuation of the supply arrangements for the UK's telecoms networks, a lack of diversity across the telecoms supply chain may impose the risk of depending on single suppliers. This in turn may further pose risks towards security and resilience of UK telecoms networks.

Digital sovereignty and technology (hardware & software)

Are there selection criteria for hardware vendors?

The UK government's "Telecoms Supply Chain Review" advises to give new restriction for the use of "high risk vendors" in the expansion of 5G and gigabit-cable networks.

This advice is that high risk vendors should be:[376]

- Excluded from all safety related and safety critical networks in Critical National Infrastructure
- Excluded from security critical 'core' functions, the sensitive part of the network
- Excluded from sensitive geographic locations, such as nuclear sites and military bases
- Limited to a minority presence of no more than 35 per cent in the periphery of the network, known as the access network, which connect devices and equipment to mobile phone masts

The UK government is currently working on legislations in order to implement the new telecoms security framework.[377] In this context, the National Cyber Security Centre has designated Chinese telecom supplier Huawei as a "high-risk vendor". In the guide published in January 2020, it is also noted that no exhaustive list of vendors exists and that operators "are encouraged" to discuss any new partnerships.[378]

In this context, it is also noted that the recent measure from the US Government to add Huawei to the US Entity List "*could have a potential impact on the future availability and reliability of Huawei's products*"[379].

374 HM Government (2016): National cyber security strategy 2016-2021, p. 51.
375 https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference.
376 https://www.gov.uk/government/news/new-plans-to-safeguard-countrys-telecoms-network-and-pave-way-for-fast-reliable-and-secure-connectivity.
377 https://www.gov.uk/government/news/new-plans-to-safeguard-countrys-telecoms-network-and-pave-way-for-fast-reliable-and-secure-connectivity.
378 https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks#section_3, Paragraph 10.
379 UK Telecoms Supply Chain Review Report, p. 7.

Furthermore, a Defence Sub-Committee is currently collecting evidence on the security of 5G an whether the UK should continue to do business with Huawei (opened March 6th 2020)[380].It is noted that existing infrastructure in the United States or Australia, which have banned Huawei and ZTE completely and have enacted bans on Huawei since 2012, is not as dependent on Huawei. In turn, Huawei has been part of the UK telecommunications infrastructure since 2003 and has been involved in building the 3G and 4G network. As the 5G network will partially sit "on top" of the existing infrastructure, getting rid of every single bit of Chinese equipment all together will bring economic and social risk and delay the 5G roll out. It is also noted that the list of international 5G suppliers is very limited.[381]

However, and despite the long-term partnership between Huawei and the UK, the evidence gathered by a Defence Sub Committee on the security of 5G is almost one sided. The only ones defending the decision to continue working with Huawei were from the government itself and from the BT Group and Ericsson, which would be the two companies to lose the most from a total ban on Huawei kit in the UK's 5G networks. Everyone else is urging the government to change its position[382]. A conclusive review has not been published yet.

Despite the review, UK's PM announced on May 22nd 2020 plans to reduce Huawei's involvement in the 5G network to zero by 2023.[383]

In November 2020, the National Security and Investment Bill was announced, which aims to strengthen the UK's ability to investigate and intervene in mergers, acquisitions and other types of deals that could threaten its national security. Furthermore, the act can be applied up to five years retroactively on deals that weren't flagged up at the time, but which now suspicious.

Possible instruments are to alter the amount of shares an investor is allowed to acquire, restricting access to commercial information, or controlling access to certain operational sites or works. There is a list of sectors deemed sensitive, many of which overlap with telecoms; Civil Nuclear, Communications, Data Infrastructure, Defence, Energy, Transport, Artificial Intelligence, Autonomous Robotics, Computing Hardware, Cryptographic Authentication, Advanced Materials, Quantum Technologies, Engineering Biology, Critical Suppliers to Government, Critical Suppliers to the Emergency Services, Military or Dual-Use Technologies and Satellite and Space Technologies.[384]

---

380 https://committees.parliament.uk/work/134/the-security-of-5g/.

381 See, e.g. https://committees.parliament.uk/oralevidence/311/default/ or https://committees.parliament.uk/writtenevidence/1873/default/.

382 See oral and written evidence: https://committees.parliament.uk/work/134/the-security-of-5g/publications/.

383 https://www.theguardian.com/technology/2020/may/22/boris-johnson-forced-to-reduce-huaweis-role-in-uks-5g-networks.

384 Telecoms.com, 11 November 2020, see https://telecoms.com/507428/uk-government-wants-to-poke-its-nose-into-telecoms-ma-in-the-name-of-security/.

Are there discussions on other technology aspects with an impact on DS?

For the public sector, the UK follows a “cloud first policy”, meaning that all organisations should evaluate cloud solutions first before considering any other option. For this, the UK government has built the Digital Marketplace, a platform that all UK public sector organisations can use to find people and technology for digital projects. The platform is currently hosted by Amazon Web Service, i.e. a US based company.[385]

Despite that the Digital Marketplace is hosted on Amazon Web Service servers, the supplier of the server or digital products sold at the Digital Marketplace are not necessarily US based. For example, the cloud provider UK Cloud with data centres based in the UK power many public sector organisations such as the UK Home Office, Department of Work and Pensions, the Cabinet Office, the Ministry of Justice, the Bank of England, NHS, etc.[386] Also, the Digital Marketplace may be seen as a vetting process of suppliers, on which third parties on the demand side make use of.

Digital sovereignty with regard to skills, norms and educational aspects

Are there (educational) programs to raise competencies, which promote DS?

The 5G Testbeds and Trials Programme is part of the 5G strategy and is targeted towards the development of a safe and secure 5G network. The program helps business to develop and embrace this technology.[387]

385 https://aws.amazon.com/government-education/g-cloud-uk/?nc1=h_ls.
386 https://ukcloud.com/why-ukcloud/.
387 https://www.gov.uk/government/collections/5g-testbeds-and-trials-programme.