Open strategic autonomy

The digital dimension

Clingendael Report

Maaike Okano-Heijmans

Clingendael
Netherlands Institute of International Relations

Clingendael

Netherlands Institute of International Relations

Open strategic autonomy

The digital dimension

Maaike Okano-Heijmans

Clingendael Report
January 2023

Disclaimer: The research for, and production of, this Clingendael Report have been conducted within the PROGRESS research framework agreement. Responsibility for the contents and for the opinions expressed rests solely with the authors and does not constitute, nor should be construed as, an endorsement by the Netherlands Ministries of Foreign Affairs and Defence.

January 2023

© Netherlands Institute of International Relations 'Clingendael'.

Cover photo: Smart city technology with futuristic graphic of digital data transfer © Shutterstock

Unauthorized use of any materials violates copyright, trademark and / or other laws. Should a user download material from the website or any other source related to the Netherlands Institute of International Relations 'Clingendael', or the Clingendael Institute, for personal or non-commercial use, the user must retain all copyright, trademark or other similar notices contained in the original material or on any copies of this material.

Material on the website of the Clingendael Institute may be reproduced or publicly displayed, distributed or used for any public and non-commercial purposes, but only by mentioning the Clingendael Institute as its source. Permission is required to use the logo of the Clingendael Institute. This can be obtained by contacting the Communication desk of the Clingendael Institute (press@clingendael.org).

The following web link activities are prohibited by the Clingendael Institute and may present trademark and copyright infringement issues: links that involve unauthorized use of our logo, framing, inline links, or metatags, as well as hyperlinks or a form of link disguising the URL.

About the Clingendael Institute

The Netherlands Institute of International Relations 'Clingendael' is a leading think tank and academy on international affairs. Through our analyses, training and public platform activities we aim to inspire and equip governments, businesses, and civil society to contribute to a secure, sustainable and just world.

The Clingendael Institute
P.O. Box 93080
2509 AB The Hague
The Netherlands

Follow us on social media
@clingendaelorg
The Clingendael Institute
The Clingendael Institute
clingendael_institute
Clingendael Institute

Email: info@clingendael.org
Website: www.clingendael.org

About the author

Maaike Okano-Heijmans is a Senior Research Fellow at the Netherlands Institute for International Relations 'Clingendael' in The Hague, where she leads the 'Geopolitics of Technology and Digitalisation' programme. She is also a Visiting Lecturer in the Master of Science in International Relations and Diplomacy (MIRD) programme at the University of Leiden

Contents

Figures

Boxes

Executive summary

In recent years the European Union (EU) and its member states hesitantly embarked on a new and ambitious path towards what came to be called 'digital and technological autonomy'. This paradigm shift involves a turn away from the market-based, open economy thinking that has dominated in European policy circles in recent decades. The new direction is towards a geostrategic, more closed economy thinking, with a shift from a focus on trade to technology.

Policies and instruments are being devised to secure public interests in the digital domain and to be resilient in an interconnected world wherein technological capability defines world leadership. This ranges from investing in telecommunications security and trusted connections, to preventing Big Tech from becoming too powerful and taking responsibility for misinformation online; and from ensuring a secure supply of the natural resources needed for microchips and batteries, to investing in digitally skilled citizens and clean and green technologies for a sustainable future. Europe's aim is to cooperate with partners, but to act based on own insights and choices.

This Clingendael Report seeks to contribute to more clarity about: (1) the interests and concerns that inform Europe's quest for digital and technological sovereignty; and (2) the instruments and policies that contribute to achieving these aims. It considers ways both to 'promote' Europe's own capabilities and competitiveness, and to 'protect' citizens against the potentially adverse effects of dependencies.

Ultimately, the EU and its member states need to develop a balanced approach to digital and technological autonomy that incorporates both 'promote' and 'protect' actions, and that is agreed and supported by all government institutions. This requires better understanding among policymakers in all ministries/institutions of the interconnections and the trade-offs among the many issues involved – ranging from stable and secure supply chains and semiconductors to competitiveness in the digital economy and internet governance. While the EU and its member states have in recent years invested in defensive action – implementing more stringent investment screening, export controls and an economic coercion instrument – policies to strengthen Europe's own technological superiority and economic competitiveness in the digital economy are still lagging.

The Digital Technology Stack as a tool

This report introduces the Digital Technology Stack (DTS) as an analytical framework to analyse the EU's and its member states' interests and concerns. It considers instruments and policies in the eleven layers of the stack. The DTS is a combination of hardware and software technologies, as well as services, that are 'stacked' on top of each other to make a device or service work.

Together, the layers of the DTS make up the totality of a country's technological capabilities, incorporating both technological and non-technological elements. The layers of the DTS are divided into three categories: (1) digital society and culture: the top three layers; (2) digital technologies and the economy (including hardware, software and services): layers four to ten; and (3) the planet: the bottom layer. Digital autonomy is about having a choice at each layer of the Stack.

Building on this initial enquiry into the European Digital Technology Stack, EU member states could consider their National Digital Technology Stacks in the EU context, combining the National DTS into a European DTS, where each member state would specialise on some parts of the stack and others on other parts. Also, there is value to considering the framework in relation to other trusted partners or adversaries. The DTS can be applied to many different case studies and can steer coordinated action between stakeholders working on specific sectors or with specific countries.

The need for a vision and strategic clarity

A whole-of-government approach that also engages stakeholders in the private sector and in civil society is needed to assure digital autonomy. Strategic clarity about what is at stake and what kind of society we want to live in will help develop a clear narrative that steers policymakers and other stakeholders in the desired direction, towards implementation.

In this age of rapid technological developments, digitalisation and global power shifts, digital autonomy concerns us all. Improved understanding of this will contribute to improved policymaking and, ultimately, to greater EU unity, strength and resilience – all prerequisites for digital and technological sovereignty and, ultimately, for European strategic autonomy.

Introduction[1]

In recent years, the parallel developments of rapid technological development, combined with global power shifts and norms divergence, have triggered a paradigm shift in the EU and EU member states. This paradigm shift involves turning away from the market-based, open economy thinking that has dominated in European policy circles in recent decades. The new direction is towards a geostrategic, more closed economy thinking, with a shift from a focus on trade to technology.

This shift includes hesitant steps on a new and ambitious path to what in the Netherlands has come to be called 'digital and technological autonomy'. Policies and instruments are being devised to uphold and enhance Europe's economic and technological competitiveness and to promote, with international partners, its ability to secure its public interests and to define rules and standards in the digital age. In other words, Europe is redefining its economic and technological sovereignty in order better to manage its economic interdependencies, reducing dependence on others without resorting to unfounded protectionism that could accelerate a geo-economic chain reaction and harm the interests of European businesses.[2]

This Clingendael Report seeks to contribute to more clarity about the concerns and interests that inform Europe's quest for digital and technological sovereignty, as well as the instruments and policies that contribute to achieving these aims. For this, it uses as an analytical framework the established conceptual model of the Stack, adapted to a Digital Technology Stack (DTS) – that is, the totality of a country's technological capabilities that include hardware, software and

1 This Report is part of a series of three publications on Dutch priorities with regard to open strategic autonomy (OSA). The Policy Brief by Luuk Molthof and Luc Köbben (October 2022) addresses OSA in the field of trade and industrial policy, while the Policy Brief by Dick Zandee (December 2022) focuses on European defence cooperation.
The author wishes to thank the policymakers, experts and other stakeholders who gave valuable feedback on the conceptual framework developed in this report.

2 Mikael Wigell *et al.*, *Europe facing geoeconomics: assessing Finland's and the EU's risks and options in the technological rivalry*, Helsinki: Finnish Government, Prime Minister's Office, 2022. Specifically, see also European Commission, *A new ERA for research and innovation*, COM(2020) 628 final, 30 September 2020.

services as well as non-technological components. The interests and instruments of the EU and its member states are unpacked in each layer of the DTS, both on the 'promote' side and the 'protect' line of action.

The DTS offers a simplified, yet comprehensive and logically structured overview of the (digital) technologies that concern multiple government agencies and officials. Presenting these in a concerted manner, in layers, will improve understanding of the full picture and the interrelations between the various layers. Highlighting both the 'promote' and 'protect' sides is to call for action that defends against unwarranted interference and that aims to enhance own capacities at the same time. While the EU and its member states have in recent years invested in defensive action, policies that invest in Europe's strength are still lagging.

By way of the DTS, this Clingendael Report seeks to contribute to improved understanding of the geopolitics of technology and digitalisation, as well as of the interconnections and trade-offs between the various elements of digital and technological sovereignty. The whole-of-government approach that is needed to tackle the interconnected economic, political and security challenges requires a higher knowledge base among all of the policymakers and stakeholders.

The DTS can facilitate conversation between a broader set of stakeholders, beyond the mostly economic specialists who work on specific subsets of the challenge on a daily basis – whether that is the digital market, semiconductor business, a secure supply of minerals or internet governance. The framework can be applied to many different case studies and can steer coordinated action between stakeholders working on specific sectors or with specific countries.

After all, only together can policymakers and stakeholders assure digital sovereignty, which is about having a choice at each layer of the Stack. Improved understanding of this will contribute to improved policymaking and, ultimately, to greater EU unity, strength and resilience. These are prerequisites for digital and technological sovereignty and, ultimately, for European strategic autonomy.

1 Europe's path towards digital and technological autonomy

Practical steps:

- Invest in greater understanding among policymakers at the national, subnational and EU levels that digitalisation – and the geopolitics of it – is a cross-cutting theme that is of relevance to all.
- Develop strategic clarity about the underlying objectives of digital autonomy – that is, the core values that we seek to uphold and the principles that we seek to defend.
- Invest in public debate about the responsibilities that these strategic objectives put on government, businesses and citizens, ensuring these are clear and broadly accepted.

The hardening competition for supremacy between the United States and China that erupted from 2017 was the first trigger for European policymakers to be more concerned with tech and digital – and the geopolitics of it. The COVID-19 pandemic exacerbated this trend, exposing digital connections as an opportunity: a life-saver, as people were suddenly forced to work, shop and interact online. At the same time, the global pandemic widened the digital divides – that is, inequalities in ability to access and use digital technologies, for example between rural and urban populations, and between small and medium-sized enterprises and big tech companies. The pandemic also exposed disruptions in the tech supply chain, which triggered a push towards so-called 'trusted supply chains' and 'friends-shoring'. The war in Ukraine that Russia started in February 2022 exposed yet further challenges to deep and strong digital connections, which were now widely used also for dis- and misinformation, hacking and (threats of) disruption of strategic infrastructures. The US elections in 2016 and the Brexit referendum in the UK had been early warnings of this, but the West started looking more seriously at these issues only now.

In operationalising digital and technological sovereignty, the Netherlands aims for open strategic autonomy (OSA) that duly considers 'proportionality' and 'openness' – and calls on the EU to do the same. A Clingendael Report of 2021 found that the twin aims of achieving strategic autonomy and preserving an open

economy are not necessarily incompatible and may even be complementary to one another.[3] Yet, a key challenge in the paradigm shift that the Netherlands and the EU are currently undergoing is to balance the inherent tension between strategic autonomy and openness, and the (potential) trade-offs between the two objectives.

European debates about digital and technological sovereignty – as subsets of OSA – really took off in 2019. For the EU and its member states, the debate is currently focusing on dependence on the dominant economic players, especially the United States and China. European Commission President Ursula von der Leyen mentioned digital sovereignty in relation to connectivity and digital infrastructure in her State of the Union speech of 2020. In that same speech a year later, she spoke of tech sovereignty – in relation to the European Chips Act, through which the EU aims to regain a 20 per cent share of global chip production by 2030.[4] Germany made digital sovereignty one of its four priorities for the digital sector during its EU Presidency in the latter half of 2020.[5] And in February 2021, Charles Michel, President of the Council of the European Union, declared: There is 'no strategic autonomy without digital sovereignty'.

In the Netherlands, digital sovereignty gained in importance under the fourth Cabinet led by Prime Minister Mark Rutte that took office in January 2022. The new Dutch government vowed to 'focus on open strategic autonomy of the EU and stimulate strength in innovation and smart industrial policy. In this way we will become leading in digitalisation and new technologies'.[6]

Since then, several new documents evidence attempts by the Dutch government to put this ambition into practice. The 'Policy Note/Strategy for Foreign Trade and Development Cooperation' of June 2022 includes digitalisation – next to sustainability – as a leading principle.[7] Also in June 2022, the 'Cyber Security

3 Luuk Molthof, Dick Zandee and Giulia Cretti, *Unpacking open strategic autonomy: from concept to practice*, Clingendael Report (The Hague: Clingendael Institute, November 2021).

4 State of the Union Addresses by President Ursula von der Leyen at the European Parliament Plenary, 2020 and 2021.

5 *Independent, inclusive and innovative: Four goals of the German Presidency for the digital sector*, eu2020.de, 24 October 2020.

6 *Coalitieakkoord 2021–2025*, 15 December 2021.

7 *Doen waar Nederland goed in is*, Beleidsnotitie BHOS 2022, 24 June 2022 (in Dutch).

Assessment, Netherlands 2022' discusses digital autonomy (and digital resilience) in a geopolitical context for the first time.[8]

While steps are being taken in various policy domains, the challenge now is to connect the dots in a coherent national agenda – laid out in the Netherlands Digitalisation Strategy (NDS).[9] Steps towards such a whole-of-government approach that contributes to OSA were detailed in a Letter to Parliament of November 2022, which emphasises the importance of greater EU resilience and that capacity to act are of paramount importance for the Netherlands to secure its public interests.[10]

The need for clarity on strategic rationale

As digital technologies are profoundly reshaping societies and the fourth industrial revolution is creating new winners and losers in economies and societies throughout the world, a growing desire to exert greater control over those technologies – that is, to operate autonomously – is only natural. But interpretations of what autonomy and sovereignty entail differ between regions and countries, as well as between stakeholders within countries. For the EU, a key challenge is to reach a shared understanding among the 27 member states. After all, only together can the EU member states reach the scale, capabilities and market power that digital sovereignty requires.

Arguably more important than debates on what exactly open strategic autonomy entails is clarity about the underlying strategic rationale. This calls attention to the more pertinent questions with regard to Europe's quest for strategic autonomy: what kind of future society do we want – specifically, in the digital domain – and how do we protect our values and the peaceful world order? This requires us to consider: (1) how we can uphold and build our own strength; (2) what is the European proposition to third countries; and (3) how can the EU deliver on this with a needs-driven approach. In other words, it requires that we not only defend or protect ourselves, but also invest in promoting our principles and values elsewhere, through regulation and the presence of our private-sector companies.

8 *Cyber Security Assessment, Netherlands 2022*, 4 June 2022.
9 For the 2022 version of the annually published Netherlands Digitalisation Strategy (NDS), see here.
10 *Letter to Parliament about Open Strategic Autonomy*, 8 November 2022.

The core values that we seek to uphold, the principles that we seek to defend and the responsibilities that these place on government, businesses and citizens must be clear and broadly accepted. Public debate, steered from the highest political level, is needed to achieve such strategic clarity and public awareness.

An important step in this direction was made in December 2022, when the Presidents of the Commission, the European Parliament and the Council signed the European Declaration of Digital Rights and Principles. The principles are shaped around six themes, namely: (1) people at the centre; (2) solidarity and inclusion; (3) freedom of choice online; (4) participation in the digital public space; (5) safety and security; and (6) sustainability of the digital future.[11]

These principles complement existing rights – such as data protection and ePrivacy – and provide guidance for the EU and its member states as they design digital rules and regulations. However, in most EU member states – including the Netherlands – discussion on these standards and principles is yet to be held with the relevant stakeholders and the broader public. Only with a strategic vision of the future society in which we wish to live can digital autonomy (and open strategic autonomy) move beyond bureaucratic jargon and be implemented with a clear narrative, acting on the shared principles of all stakeholders.

Actual steps towards technological and digital sovereignty need to be taken at the national, subnational and EU levels. These steps can then be measured against the agreed standards, and any potential undermining of the benefits of the global market, international trade, international social interactions and accompanying investments can be avoided.[12]

Digital and technological sovereignty, or autonomy?

Academics and experts have intensely debated the concepts of autonomy, sovereignty and resilience – with prefixes, such as 'open' (hence, OSA), 'military', 'digital', 'tech' and 'data'. Government agencies, however, appear to be rather pragmatic in the terminology they use. For example, while the Dutch security

11 European Commission, *Declaration on European Digital Rights and Principles*, Brussels, 15 December 2022.

12 See also NLdigital.

establishment uses the term 'digital autonomy', until recently the Dutch Ministry of Economic Affairs and Climate adhered to 'digital sovereignty'. Digital resilience is a term used by officials in both the economic and security establishments.

Digital sovereignty or autonomy is considered to be a subset of open strategic autonomy – or, as the Dutch Cyber Security Council (CSR) puts it: 'strategic autonomy in the digital domain'. The Netherlands Coordinator for Counter-terrorism and Security (NCTV) describes it as: 'the ability and the means that the Netherlands has to autonomously take decisions about (further) digitalisation as well as the desired level of digital resilience'.[13]

Recognising that there is not one unambiguous definition of digital autonomy or sovereignty, this Clingendael Report follows the definition of OSA presented in the Letter to the Dutch Parliament, tweaked to the digital domain in line with the Ministry of Economic Affairs:

> EU digital autonomy concerns the ability – as a global player, in cooperation with international partners, based on own insights and choices – to secure public interests in the digital domain and to be digitally resilient in an interconnected world.[14]

This report engages mainly with two elements of this definition: 'own insights and choices'; and being 'digitally resilient in an interconnected world'. It does so by unpacking interests and concerns, as well as instruments and tools to act on those concerns, using the Digital Technology Stack as an analytical framework. This concurs with the argument of the European Digital SME Alliance that the EU and its member states 'need to define the level of independence and needs for own technologies for each of the layers of the technology stack, with the aim to offer free choice where this is essential'.[15] This analytical framework also offers clarity into the capabilities and assets that are required for digital sovereignty. These include natural resources, critical infrastructures, data availability and usage, standardisation and interoperability, digital skills and cyber security.

13 Cyber Security Raad (CSR), *Advies 'Nederlandse digitale autonomie en cyber security'*, May 2021; and NCTV, *Cybersecurity Beeld Nederland*, 2022, p. 8.

14 *Letter to Parliament*, November 2022, p. 3; and unpublished 'think piece' on digital sovereignty by the Ministry of Economic Affairs, January 2022.

15 European Digital SME Alliance, White Paper on digital sovereignty, 27 October 2021, pp. 4–5.

2 The DTS as an analytical framework

Practical steps:

- Use and further develop the Digital Technology Stack (DTS) as a conceptual framework and policy tool to: (1) improve understanding of the many issues at stake and how they interrelate; (2) facilitate discussion and improved understanding among policymakers in all government institutions about digital autonomy.
- Recognise and act on the fact that digital autonomy requires policies and instruments that both protect and promote European and EU member states' national interests.
- Invest in dialogues with key stakeholders in Parliament, the private sector and non-governmental organisations that facilitate policy outcomes that balance both elements.

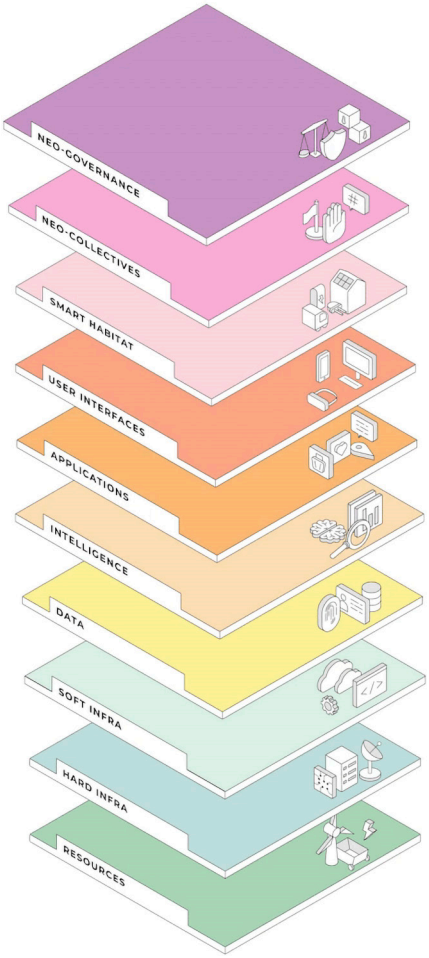
Achieving digital autonomy requires that this broad concept is understood by and manageable for any single policymaker charged with implementing part of it. While any single action towards digital autonomy may be challenging as such, the even bigger challenge is to act with awareness of the bigger picture so as to ensure that interlinkages between various policies are established as needed.

Aiming to contribute to better understanding of the interconnections and the trade-offs between the various elements of digital and technological sovereignty that are needed for integrated policymaking, this report employs the well-established concept of the Stack.[16] More specifically, it proposes the Digital Technology Stack (DTS), which builds on the Stack model developed at FreedomLab think tank that presents digital technology as a layered structure of technological and non-technological components (see Figure 1 below).[17]

16 Engineers will be more familiar with the Open Systems Interconnection (OSI) model, which describes the seven layers that applications use to communicate over a network.

17 See *Toekomstverkenning digitalisering 2030* (paper prepared by FreedomLab), 26 April 2021, pp. 21–22; and Sebastiaan Crul, *An introduction to the Stack*, FreedomLab, 29 March 2022. See also Claire Stolwijk *et al.*, Bridging the Dutch and European digital sovereignty gap, TNO Report, TNO 2022 R10507, March 2022.

Figure 1 The Stack: technological and non-technological components



Source: Sebastiaan Crul, An introduction to the Stack, FreedomLab, 2022

Although the concept of the stack is relatively new to political scientists, to engineers it is common to speak of technology stacks. A stack is a combination of hardware and software technologies, as well as services, that are 'stacked' on top of each other to make a device or service work. This may be a mobile phone or electric vehicle, cloud computing or e-commerce. For each of those products to operate requires resources, software and applications, among other things.

Incorporating both technological and non-technological elements in the stack allows for a better understanding of the geopolitical impact of digital technology. This transforms the traditional engineering stack model to a framework that is more appropriate for political science analysis. It also makes the model more tangible as a tool for analysis and strategic decision-making at the national (or EU) level.

Box 1, below, details the eleven layers of the Digital Technology Stack, divided into the three categories of: (1) digital society and culture: the top three layers; (2) digital technologies and the economy: layers four to ten; and (3) the planet: bottom layer. The DTS proposed here adds an eleventh layer of 'planet' to the Stack shown in Figure 1, to account for the fact that planetary security and sustainability underpin all of the above. Also, it makes the model more useful for action by highlighting interests and concerns, as well as policies and instruments in both the 'promote' side and the 'protect' line of action.

Unpacking the concept of digital autonomy through the DTS will highlight in which layers of the stack value creation takes place, who owns these value creating assets, and hence, who can wield power in specific layers of the stack. The DTS will thereby help countries to recognise strengths and dependencies for their digital infrastructures, applications and services in each layer of the Stack. This is important because, as highlighted by the Dutch organisation for applied scientific research TNO, the Netherlands and Europe currently have insufficient insight into these new dependencies, which is a challenge to pursuing sufficiently proactive coordinated policy solutions. For example, the greater implications for digital sovereignty will be missed with an excessive focus on cyber resilience.[18]

Box 1. Layers of the DTS, briefly explained

Top three layers: digital society and culture

Neo-governance	New forms of governance that have arisen as a consequence of the digitalisation of society.
Neo-collectives	New cultural practices and communities, both physical and virtual, that have arisen as a consequence of the digitalisation of society.
Smart habitat	New environments where devices are central to human interactions. Smartphones are core to these

18 Claire Stolwijk *et al.*, Bridging the Dutch and European digital sovereignty gap, TNO report, TNO 2022 R10507, March 2022.

	environments, as they carry the ability (via apps) to function as a wallet, monitor vital signs, and to function broadly as a data collector and execute tasks that were not possible until very recently.
Central layers four to ten: digital technologies and the economy	
User interfaces	Set of ways that an end-user has to communicate and interact with an application. Interfaces are mostly visual but can also be based on speech or movement. Highly influenced by behavioural psychology.
Applications	Allow the end-user to access, manipulate, manage, organise, retrieve or update the information required to perform a certain functionality. They provide the actual services to be offered to the end-user.
Intelligence	Related to the ability of a certain algorithm or application to learn user behaviour, enabling optimisation and personalisation.
Data	Data required to perform a certain strategic, business or operational function. This may consist of metadata (i.e. data about data), business data, personal data and other data types.
Soft infrastructure	Virtual elements, built on top of the hard infra-structure, that allow for virtualisation of hardware, middleware, databases, operating systems and hardware management. Cloud providers offer more and more of these solutions as a service.
Hard infrastructure	Hardware elements, also known as physical infra-structure. This includes hardware storage, computing power, sensors, batteries, chips, screens and transmission elements, such as cables and antennas.
Resources	Physical elements that constitute the material component of our digital devices and infrastructure. These include standard as well as rare and man-made elements.
Bottom layer: environment	
Planet	Source of all natural, physical and human resources. All conversations and action related to technology and digitalisation need to consider the impacts on planetary security and sustainability.

Ultimately, the purpose is to reach a 'National DTS' – here understood as the layered set of technologies and capabilities that together define a nation's capacity for autonomous decision-making and action in the digital age – that is, a nation's technological and digital sovereignty.[19] Linking elements of digital autonomy to specific layers of the DTS can help ensure that policymakers acknowledge and act on challenges and opportunities in each layer of the Stack, as well as the interplay between developments on different layers. For example, if (too) much power is concentrated with one company that is active in one layer of the DTS, this may push that company to operate also in other layers of the DTS and become even more powerful. Understanding the full picture is key to avoiding compartmentalisation when acting on specific elements of digital sovereignty.

As a next step, EU member states should consider their National DTS in an EU context, combining their National Digital Technology Stack into a European DTS, where each member state would specialise on some parts of the Stack and others on different parts. Much like in the field of defence, where attempts have been made in recent years to pool EU member states' resources, this will surely be challenging in theory and in practice. Nevertheless, a truly collective approach – not just in strategy but also in capabilities – should be a dot on the horizon that should be considered for effectiveness and efficient use of limited resources.

Courses of action: protect, shape and regulate, promote

Digital sovereignty is thus about having a choice at each level of the Digital Technology Stack.[20] Ensuring choice involves a delicate balance of policies that either protect or promote European digital interests, principles and rights. As such, digital sovereignty is about: (1) the 'protect' element: addressing dependencies and vulnerabilities in order to improve resilience; (2) the 'shape and regulate' element, or digital governance: regulating at both the national and international/European levels, as well as introducing numerous public and private-sector mechanisms to steer technology developments and deployment;[21]

19 This draws on Markus Holmgren, *Autonomy through digital resilience: the importance of upholding the national tech stack*, FIIA Briefing Paper no. 341, 9 June 2022.

20 European Digital SME Alliance, White Paper on digital sovereignty, 27 October 2021, p. 9.

21 Lawrence B. Solum, *Models of internet governance*, Illinois Public Law Research Paper no. 07-25, 2008.

and (3) the 'promote' element: strengthening and steering societies through trade, investments and attraction, and making use of capabilities in equipment, personnel, information and capital. As visualised in Figure 2 below, the 'shape and regulate' element overlaps with the other two elements, 'protect' and 'promote', signifying the fact that it enables and potentiates them.[22]

Figure 2 Three courses of EU action

Source: author's compilation

A successful whole-of-government approach to digital autonomy considers these three fields in an integrated manner. In practice, however, this often does not happen. This is illustrated by the fact that European policies of recent years have largely focused on the 'protect' side – that is, on trade defence instruments and protection of critical infrastructures – while real steps in the flagship initiatives on the 'promote side' – that is, innovation and valorisation policies and the EU's Global Gateway project – are lagging. This is problematic, as it is ultimately the 'promote' side that will leverage and unlock the potential that Europe has and needs to realise digital autonomy.

In order to address this deficiency, the following sections consider key concerns and interests on both the 'promote' and 'protect' sides. 'Shape and regulate' elements are incorporated on either side, in order to simplify the analysis somewhat.

22 It deserves mentioning that the distinction between 'promote' and 'protect' is not always clear, and policies and instruments in both fields clearly overlap. They are two sides of the same coin.

3 Towards implementation: the European DTS

Practical steps:

- Regularly finetune and update the European Digital Technology Stack to track key developments in the field and European responses to them.
- Ensure an appropriate balance between protect and promote policies in the DTS.

This report makes a first step towards a European Digital Technology Stack (EDTS) by unpacking interests and concerns, as well as policies and instruments in each layer of the Stack. The figures below present the outcomes of this exercise at the European level.

Concerns and interests

Figure 3, below, summarises key concerns and interests of European digital sovereignty at the EU level. Having this comprehensive overview is important to ensure that the relevant stakeholders know and agree on what is at stake and why action is needed. Such strategic clarity will build a clear narrative to help steer policymakers and other stakeholders in the desired direction, towards implementation.

Consider, for example, the complex domain of data. Data privacy is a fundamental concern and interest on the 'protect' side, while data ownership and portability are on the 'promote' side. Data privacy is mentioned in the non-technological 'smart habitat' layer within the category of digital society and culture, as well as in the technological layer of 'user interfaces'. This calls attention to the issue of data-gathering and the use of those data in smart cities. However, concerns over data privacy can and must also be addressed at an earlier stage of technological development – that is, a few layers down in the DTS, in the 'data' and 'soft infra' layers. For example, decentralised finance (DeFi) provides a decentralised, soft infrastructure that enables data-sharing and data ownership. Greater awareness among a larger group of policymakers on this can contribute to investments into

optimal use of technological solutions to address concerns and interests, while mitigating the challenges.[23]

Figure 3 Unpacking the European Digital Technology Stack: concerns and interests of digital and technological sovereignty

	Layer of the DTS	Protect		Promote
Digital society and culture	Neo-governance	Decentralisation, open source	Digital diplomacy and trusted connectivity	Digital principles and rights
	Neo-collectives	Civic organisation		Multistakeholderism, digital participation, decision-making and enforcement
	Smart habitat	Data privacy		Digital government (G2C, G2B), ownership of digital ID and finance, (green and) smart cities, smart health
(Digital) technologies and economy	User interfaces	Data privacy: voice assistant, 3D cameras		Digitally skilled citizens
	Applications	New dual-use technologies, dis- and misinformation, election interference		European platform companies (email, social media, fintech, etc.)
	Intelligence	Access to 'smart' algorithms		High performance computing and AI
	Data	Data privacy, espionage		Data ownership and portability
	Soft infrastructure (operational)	Control over essential service providers: cloud software, internet protocols		Interoperability of data and services, technical standards-setting, human capital
	Hard infrastructure (physical)	Integrity and control of critical infrastructure: cyber attacks		European telecommunications companies (5G+), cloud services, semiconductor industry
	Resources	Supply chains security: energy, raw materials, rare earths		Ownership of critical technologies and products, stable supply of electricity
Environment	Planet	Sustainable habitat		Green technologies/transition

Note: G2C: government to citizen; G2B: government to business; AI: artificial intelligence

Source: author's compilation

23 For more on this, see *The geopolitics of digital financial technologies: a chance for Europe?*, Clingendael Report, January 2022.

The concerns and interests mentioned in Figure 3 are, of course, not of the EU and its member states alone – they are shared by the EU's trusted allies. In highlighting the fact that these concerns are acted upon not only with 'EU-only' initiatives but also with partners, digital diplomacy and trusted connectivity are incorporated throughout the DTS in a vertical, cross-cutting way.

EU Digital Diplomacy was formally launched in July 2022 with the aim 'to secure the EU global role in the digital world, to protect its strategic interests and to promote its dynamic, human-centric regulatory framework for an inclusive digital transformation'.[24] One specific concern that it acts upon is an open and secure internet. The Declaration on the Future of the Internet of April 2022 is the first successful example of EU cooperation with the United States in this regard.[25] An early draft of the Declaration risked contributing to fragmentation of the global internet, focusing more on sanctioning the internet – for example, internet infrastructure organisations suspending certain members or internet governance institutions imposing barriers on access to a free and open internet in certain regions. This draft was successfully steered towards a positive vision for an 'open, free, global, interoperable, reliable and secure' internet, endorsed by a diverse group of 60 countries from all continents.

The push for so-called 'trusted connectivity' originates mainly from Estonia, which since 2017 has hosted the annual Tallinn Digital Summit, focusing in 2022 on this very issue.[26] The essence of trusted connectivity is to do business with partners according to common interests, democratic values and the highest regulatory and social standards. Incorporating both 'protect' and 'promote elements', trusted connectivity is instrumental to ensuring geopolitical stability, a successful digital and green transformation, and economic and energy security. Acting on these interests, the EU in 2022 forged Digital Partnership Agreements (DPAs) with Japan and Singapore, and is seeking to establish more such partnerships, including with South Korea.

24 European External Action Service, *Digital Diplomacy*; and *Council conclusions on digital diplomacy*, 18 July 2022.

25 *EU and international partners put forward a Declaration for the Future of the Internet*, Brussels: European Commission, 28 April 2022.

26 *Tallinn Digital Summit*, 10–11 October 2022. See also the *Asia–Europe Sustainable Connectivity (AESCON) conference and Policy Brief series*, 22–24 March 2022.

Instruments and policies

Building on this understanding of concerns and interests at the European level, the next step is to assess where the EU and its member states stand in devising policies and instruments to promote those interests. For this purpose, Figure 4 presents the instruments and policies that are implemented and in the making, as well as known topics that have yet to be addressed. Highlighting these 'known unknowns' also serves the purpose of identifying so-called 'unknown unknowns': concerns and policies that are not yet known but that ought to be addressed. Box 2, also below, adds a brief explanation of the EU initiatives mentioned (as acronyms) in Figure 4.

The different colours in Figure 4 highlight whether specific instruments are in place, in the making or early stages of implementation, or not yet on the agenda. For example, in the top layer of the 'digital society and culture' category, since 2018 the European Commission's Next Generation Internet (NGI) initiative has been dedicated to shaping the development and evolution of the internet into an 'Internet of Humans', contributing to the open source community. By comparison, the Gaia-X project, which seeks to enable the transition to composable, interoperable and portable cross-sector data sets and services, is in an earlier stage of operations. This project is governed by the Gaia-X Association, which was founded in 2021 by 22 companies and has over 340 members today. All other initiatives in this same category are also at this early phase of implementation.

By comparison, the EU and its member states are at a far more advanced stage of development than other countries and jurisdictions, with several policies and instruments in the (digital) technologies and economy category. For example, in the field of data governance, the General Data Protection Regulation (GDPR) represents Europe's first success in global standard-setting in the digital domain. The EU is now seeking to replicate this success with the Digital Markets Act (DMA) and Digital Services Act (DSA), which entered into force in November 2022. Other regulatory and industrial policy initiatives that seek to protect and promote European interests are still in the making.

Figure 4 Unpacking the European Digital Technology Stack: instruments and policies acting on digital and technological sovereignty

	Layer of the DTS	Protect		Promote
Digital society and culture	Neo-governance	Trusted communities	Digital diplomacy and trusted connectivity	Next Generation Internet (NGI) Open internet Gaia-X Association
	Neo-collectives	Hacktivism		Public–private–people partnerships, sandbox programmes, hacktivism, digital principles and rights
	Smart habitat	Cyber Resilience Act		Internet of Things (IoT) European digital identity
(Digital) technologies and economy	User interfaces	General Data Protection Regulation (GDPR)		European digital identity
	Applications	Digital Markets Act (DMA), Digital Services Act (DSA) Export controls		Multilateral e-commerce rules Digital euro
	Intelligence	AI export controls		AI Act
	Data	GDPR Data Governance Act		Data Act, OPEN DEI Initiative, International Data Spaces (IDS), Blockchain Strategy
	Soft infrastructure (operational)	Foreign Direct Investment (FDI) screening, Cybersecurity Certification Scheme for Cloud Services Outbound Investment Screening		Gaia-X, Web3 technologies (incl. edge computing, decentralised finance), European digital identity, Digital for Development (D4D)
	Hard infrastructure (physical)	5G Toolkit, NIS Directive, Cyber Security Act Government/public procurement, Quantum FDI screening Outbound Investment Screening		Global Gateway (telecom networks, cables, satellites), Digital for Development (D4D) Quantum technology, Mobile telecommunication standards (6G)
	Resources	Economic coercion tool, Interdependence inventory, Resources Strategy, Critical Raw Materials Act		Trusted Supply Chain Forum, European Chips Act, European Battery Alliance
Environment	Planet	European Green Deal (EGD)		European Green Deal (EGD) European Green Digital Coalition

Note: The image shows policies and instruments in place at the EU and EU member-state level (green); in the making or early stages of being implemented (orange); and not yet on the agenda (red)[27]
Note: Policies and acronyms are explained in Box 2.

Source: author's compilation

27 Note that the colour does not say anything about the effectiveness of a specific policy or instrument.

Box 2. EU initiatives, briefly explained

AI Act	**Artificial Intelligence Act** – EU regulation that aims to regulate the use of AI, using a risk-based approach with four layers and corresponding regulation, ranging from 'unacceptable risk' to 'minimal or no risk' applications.
DGA	**Data Governance Act** – EU regulation that aims to increase trust in data-sharing, make more data available and facilitate data-sharing across sectors and EU countries.
Data Act	EU regulation that complements the DGA and aims to establish rules regarding the use of data generated by Internet of Things (IoT) devices, ensure certainty about data rights and encourage more actors to participate in the data economy.
DMA	**Digital Markets Act** – EU regulation that aims to ensure integrity in digital markets, by enforcing fair behaviour by very large online platforms (entered into force in 2022).
DSA	**Digital Services Act** – EU regulation that aims to provide better protection for internet users and their fundamental rights, by enforcing accountability of online platforms on illegal and harmful content (entered into force in 2022).
EGD	The **European Green Deal** aims to move to a cleaner and circular economy, to stop or delay climate change.
Gaia-X	European initiative to develop federated data and cloud infrastructure. The Gaia-X European Association for Data and Cloud represents the core of the organisational structure.
GDPR	**General Data Protection Regulation** – EU regulation that aims to safeguard personal data and uphold the privacy rights of EU citizens (in effect since mid-2018).
IDS	**International Data Spaces** – Industry-led initiative that aims to create a technical standard for open, transparent and self-determined data exchange, a central element of the Gaia-X project.
NGI	**Next-Generation Internet** – European Commission-led initiative that aims to shape the development of the human-driven internet of the future, reflecting European values and norms.

NIS Directive	**Directive on Security of Network and Information Systems** – EU-wide cybersecurity legislation aiming to enhance cybersecurity across the EU bloc.
Open Internet	EU rules enshrine the principle of open internet access: internet traffic shall be treated without discrimination, blocking, throttling or prioritisation.
OPEN DEI	**Open Digitalisation of European Industries** – EU-funded initiative that aims to close the gaps and encourage synergies across regions, nations, sectors and actors working on the Innovation Actions implementing the EU Digital Transformation strategy.

When considered comprehensively, Figure 4 highlights several important points. First, while the EU and its member states have started to act on a variety of interests and concerns related to digital autonomy, much of that remains work in progress. This goes in particular for the 'promote' line of action, where Global Gateway projects and D4D initiatives are still in the making.[28] Moreover, several issues are not yet on the agenda but appear on the horizon because other key players are acting on them. These include outbound investment screening and export controls on artificial intelligence, pushed for in the United States; and a digital euro, particularly in view of China's steps towards a central bank digital currency.

Second, several initiatives appear in different layers, for having both technological and non-technological transformative elements. For example, Gaia-X must be considered not just as a European cloud initiative that seeks to promote a European software alternative to currently mostly US cloud offerings; it also proposes an alternative governance model of open-source and decentralised solutions wherein technology innovators are building a radically new, global and open-source infrastructure. The same can be said of a European digital identity, which creates soft infrastructure with immediate links to how governments and citizens can communicate and interact with each other.

28 Investments are starting to be made, including in the Medusa optical-fibre submarine cable to connect Northern African countries to Southern European countries; the extension of the submarine and terrestrial fibre-optic cable BELLA to Central America and the Caribbean; and the establishment of Earth Observation Centres in Panama and the Philippines through 'Copernicus'. See European Commission, December 2022.

Third, the digital and green transitions are intrinsically interrelated. Efforts towards each should go hand in hand and must be seen in tandem, not just from a policy perspective but more fundamentally because planetary security is a prerequisite for both. Also here, agreed standards and principles that are shared and supported by all stakeholders should steer action, rather than policy objectives decided by elites and imposed in a top–down manner. The European Green Digital Coalition is an example of this approach being tested in practice.

4 The way forward: priorities and policy recommendations

Practical steps:

- Use the National Stack to map the political landscape – that is, to identify convergences and divergences in interests, priorities and policies of EU countries and key EU partners in the digital domain.
- Establish regulatory dialogues between trusted communities, both in a Track 1.5 setting and through a multistakeholder approach, to identify the potential for convergence of principles and policies between EU member states and of the EU with its partners.

The unpacking of the European Digital Technology Stack (EDTS) can facilitate the process of digital autonomy creation in a variety of ways. First, as a comprehensive overview pointing also to interlinkages between different layers of the Stack, it can facilitate discussion between policymakers that specialise in any given part of it. Second, it can help identify gaps in strategic thinking and policymaking, by forcing policymakers to consider all layers and all sides of the model. Third, the EDTS can help in moving from theory to practice and can assign budget and projects to areas of the Stack where an EU member state or the EU itself is falling behind.

Taking this one step further, the EDTS may be unpacked at the EU member state (that is, national) level and the EU level, making it a tool to highlight where the EU and individual EU member states stand on their way to these aims – implementing European regulations and guidelines. It could also facilitate mapping of the political landscape, if third countries are mapped in this similar way. The EDTS can then unveil opportunities and obstacles to coordination or cooperation between (groups of) countries and thereby contribute to the creation of political coalitions.

Such use of the EDTS may add clarity to how index measures of countries' technological capabilities and their commitment to technological sovereignty relate. Such indices include, first and foremost, the Digital Economy and Society Index (DESI, the EU tool that summarises indicators on EU countries' digital

performance and tracks progress), but also the European Sovereignty Index developed by the think tank European Council on Foreign Relations.[29]

Linked to this, the Stack model can help to identify European champions (at the country, sectoral and company level), or to build consortiums of countries to assist one another with digital governance and development. For example, as a champion of public services digitalisation, Estonia could help others with government e-identity in various layers highlighted in the EDTS. And the Netherlands can appeal for the need to discuss export controls in semiconductor business at the European level, highlighting how this is a cross-cutting issue in various layers of the Stack that should be a concern for all – and not just those active in the semiconductor ecosystem. The EDTS can also help in identifying all too powerful companies that are active in one layer of the Stack, and sound the alarm if these companies move towards operations also in other layers of the Stack – which might otherwise lead to too much concentration.

29 European Commission, *The Digital Economy and Society Index*; and Jana Puglierin and Pawel Zerka (eds), *European Sovereignty Index*, Brussels: European Council on Foreign Relations, June 2022.

Conclusion: digital autonomy as a concern for all

In recent years the EU and its member states hesitantly embarked on a new and ambitious path towards what came to be called 'digital and technological autonomy' – that is, the capacity for autonomous decision-making and action in the digital age. The Digital Technology Stack (DTS) proposed in this Clingendael Report unpacks the layered set of technologies and capabilities that together define a nation's digital autonomy. The DTS clarifies how the many elements of the digital technology field interrelate and makes digital autonomy realistic, highlighting the need for action on both the 'protect' and 'promote' lines of action.

As such, the Digital Technology Stack offers clarity for policymakers who are not active with tech or digital issues on a daily basis, but who understand that digital autonomy cannot only be left to economic specialists. Seeing the full picture is the key to avoiding compartmentalisation that may arise as policymakers focus on specific issues areas, policies or instruments in any one layer of the Stack. Moreover, a comprehensive view will help avoid an overly excessive focus on policies and instruments that either seek to enhance autonomy by reducing vulnerabilities ('protect') or to ensure competitiveness ('promote') when striving for specific elements of digital autonomy.

Building on this initial enquiry into the European Digital Technology Stack, there is value to considering it at the national level, EU-wide level, and in relations with other trusted partners or adversaries. The framework can be applied to many different case studies and can steer coordinated action among stakeholders working on specific sectors or with specific countries.[30]

In this age of rapid technological developments and digitalisation, digital autonomy concerns us all. A whole-of-government approach that engages stakeholders in the private sector and in civil society is needed to assure

30 A first attempt at this is made in a forthcoming publication on EU–China dependencies and digital autonomy; see Maaike Okano-Heijmans, *Europe's strategic dependencies on China: the digital domain*, EU and China Think Tank Exchanges compilation, Brussels: European Policy Centre (EPC), January 2023.

digital sovereignty, which is about having a choice at each layer of the Digital Technology Stack. Improved understanding of this will contribute to improved policymaking and, ultimately, to greater EU unity, strength and resilience – all prerequisites for digital and technological sovereignty and, ultimately, for European strategic autonomy.