

Strengthening digital economic security in Europe

Promote, Shape, Regulate and Protect, please!

Maike Okano-Heijmans
Alexandre Gomes
Daniel Kono

Clingendael Report



Clingendael

Netherlands Institute of International Relations



Clingendael

Netherlands Institute of International Relations

Strengthening digital economic security in Europe

Promote, Shape, Regulate and Protect,
please!

A study for the Dutch Ministry of Economic Affairs and
Climate Policy

Maaïke Okano-Heijmans
Alexandre Gomes
Daniel Kono

Clingendael Report
October 2023

Disclaimer: The research for, and production of, this Clingendael Report have been conducted for the Netherlands Ministry of Economic Affairs and Climate. 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 Ministry of Economic Affairs and Climate.

October 2023

© Netherlands Institute of International Relations 'Clingendael'.

Cover photo © Clingendael Institute

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](https://twitter.com/clingendaelorg)
-  [The Clingendael Institute](https://www.linkedin.com/company/the-clingendael-institute)
-  [The Clingendael Institute](https://www.facebook.com/TheClingendaelInstitute)
-  [clingendael_institute](https://www.instagram.com/clingendael_institute)
-  [Clingendael Institute](https://www.youtube.com/channel/UCgk8LW131t8U3XU01D0100g)

Email: info@clingendael.org

Website: www.clingendael.org

About the authors

Maike 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) of the University of Leiden.

Alexandre Gomes is a Research Fellow at the Netherlands Institute for International Relations 'Clingendael' in The Hague, where he is part of the EU & Global Affairs Unit and of the 'Geopolitics of Technology and Digitalisation' programme. His research focuses on the role of technology in geopolitics.

Daniel Kono was a research intern at the Clingendael Institute in February–August 2023.

Contents

Executive summary	1	
Abbreviations and acronyms	5	
List of tables	7	
List of figures	8	
Introduction	9	
1	Explaining the turn to DOSA and economic security: geopolitical catalysts and policy shifts	13
1.1	Three key catalysts for the ongoing policy shifts	13
1.2	Strategic questions for the coming decades	16
1.3	Relevant partnerships	19
2	The European and Dutch approaches to the digital dimension of strategic autonomy	31
2.1	Europe's digital decade?	31
2.2	The Dutch turn to DOSA	34
2.3	Concluding remarks	38
3	Partners, rivals and best-practice countries	39
3.1	The Digital Technology Stack	39
3.2	Quick scan: partners and rivals in an evolving geopolitical landscape	42
3.3	Analysis of EU member states	52
3.4	Analysis of non-EU countries	69
3.5	Concluding remarks	89
4	Towards digital resilience and autonomous choices: actionable steps	91
4.1	The Netherlands as an EU member state	93
4.2	Cooperating and dealing with third countries	98
4.3	In focus: Promote	102
4.4	In focus: Protect	106
4.5	Concluding remarks	108

Executive summary

Increased geopolitical tensions and accelerated technological shifts are forcing governments to turn their focus to technology and digitalisation. Technological leadership, digital autonomy and economic security are now political Chefsache in countries throughout the world, including in Europe. Obtaining, managing and using data for commercial gains is increasingly important as new technologies, such as artificial intelligence, are revolutionising industries and reshaping societies.

Set against this context, the Dutch government is preparing implementable measures to act on open strategic autonomy (OSA) in the digital domain, to be presented during autumn 2023. This comes just months after the launch of the European Economic Security Strategy by the European Commission. The Dutch government must reckon with the move in this new direction – from DOSA to (digital) economic security – if it wishes to leverage its reputation as a European frontrunner in this field.

This report offers a strategic international analysis to inform Dutch policies and action on digital economic security, in a European context. It reflects on the geopolitical context that shapes digital OSA (DOSA) concerns; showcases the key features of both the European and Dutch approaches to the digital component of strategic autonomy; presents a concise overview of the state of play in a select group of key countries; and offers suggestions for future action. A key point emerging from the report is that, in seeking to enhance their digital OSA, European governments need to ensure that they act on two lines of action: Promote and Shape policies; and Regulate and Protect. The focus on Regulate and Protect of recent years must be complemented by greater investments in Promote and Shape policies – both within the European Union and in coordination with key partners.

Actionable steps for Dutch policymakers

In order to ensure open strategic autonomy in the digital domain, the Netherlands needs to act, ideally aligned with the EU and its fellow member states. The following practical steps emerge from this report's analysis.

Networks and partners

- **Pick your partners.** Co-create with 'Digital Partners', communicate with 'Friendly Competitors' and captivate 'Potential Converts' and 'Analogue Challengers'.
- **Multilateralism where possible; unilateralism where needed.** Aim to keep international dialogue and consensus at the highest level possible. For strategic themes (such as semiconductors and quantum technologies), engage in sectoral unilateral settings to enable focused collaboration with partners that share Europe's interests, such as India, Japan, the United States, South Korea and Taiwan.
- **Share Dutch best practices (Shape).** Using the networks of attachés responsible for innovation, economic security, cyber, and education and science at Dutch embassies worldwide, proactively share best practices with the EU and other member states to shape their course.
- **Do not run alone; be mindful of other EU member states.** Invest in an inclusive approach on issues where the Netherlands has a unique position, such as export controls on semiconductor equipment, to increase the likelihood of getting EU partners on board with a desirable direction.
- **Involve and support the private sector and civil society.** Act on the understanding that, ultimately, it is European companies – large and small – and citizens who will feel the consequences of the new economic security agenda.

Best practices learned from other countries

- **Engage with the industrial policy practices of France and Germany.** Engaging with German and French willingness to support industrial policies that nurture the growth of high-tech and digital firms can help attract investments and entrepreneurship to EU member states.
- **Learn from Finland's long-standing public-private cooperation on the security of supply of resources.** The Finnish approach of voluntary, structural and mutually beneficial public-private cooperation to ensure the security of supply holds important lessons for the Netherlands to engage the private sector.

→ **Learn from the US's targeted cooperation on tech and digital in minilateral settings.** EU and Dutch strategic cooperation on technology and digital issues with third countries should be taken beyond bilaterals towards sectoral and minilateral cooperation with key countries, when needed.

→ **Learn from China's Shape approach.** Delivering on digital projects of substantial scale and impact are requirements to raise the Dutch and EU's international profile and credibility with partner countries in the Global South. Leverage expertise in areas such as cybersecurity to create new international standards in this domain that reflect European values.

→ **Learn from the India Stack initiative.** Dutch and European tech and digital firms should investigate how to benefit from the India Stack initiative, both as a best practice to implement at home, as well as a basis to access the world's biggest market.

Parallel lines of action: Promote and Shape–Regulate and Protect (PS–RP)

→ **Diversification and back-up plans are needed in all layers of the Digital Technology Stack.** Vulnerabilities stemming from dependencies on in-depth, integral digitisation using technology that is managed and developed by foreign parties predominate. Analogue back-up plans thus need more attention.

→ **Promote at home.** The turn to smart industrial policy is certain but painful. To project the image of being a constructive engager, the Dutch government can focus on structural reforms that enable a thriving digital ecosystem as well as on ensuring a market for investments by engaging end-users in investment programmes.

→ **Promote and Shape abroad.** Concrete steps are still lagging, especially when compared to the rapid adoption of Protect instruments. The Netherlands and the EU thereby risk losing important allies that are needed for success in DOSA: the private sector and emerging economies.

→ **Protect measures are more successful if adopted by more countries.** Greater investments are needed to engage also less-like-minded countries on Protect measures. This requires engagement with those countries on their terms,

and prioritising concrete, quick wins alongside incremental progress on large and complex sets of measures.

→ **Companies and academic institutions must be enticed to act on economic security.** New instruments are needed to develop relationships of trust among public, private, academic and nonprofit stakeholders.

Tactics

→ **In the EU context, move beyond battles of words to focus energy and attention on action.** Engage with the turn towards economic security and de-risking, reformulating the DOSA narrative in terms of Digital Economic Security.

→ **Ensure that risks posed by new (digital) technologies feature in economic security.** Steer attention to the risks of new technologies to fundamental rights such as freedom of expression, privacy and human dignity to strengthen the economic security strategy's digital element.

→ **Develop strategic clarity about the objectives of autonomy in the digital domain.** Develop a joint vision for the future digital society, through dialogues with the private sector and civil society, to ensure that all stakeholders are on board with the new direction.

Abbreviations and acronyms

AI	Artificial intelligence
API	Application programming interface
ASEAN	Association of South-East Asian Nations
ASPI	Australian Strategic Policy Institute
BIS	(US) Business of Industry and Security
BOSS	(India's) Bharat Operating Systems Solutions
BRI	Belt and Road Initiative
BPM	Business process management
CBERS	China–Brazil Earth Resources Satellite
C-DAC	(India's) Centre for Development of Advanced Computing
CRM	Critical raw materials
D4D	Digital for Development
DEPA	(India's) Data Empowerment and Protection Architecture
DES	Digital economic security
DESI	Digital Economy and Society Index
DG CONNECT	Directorate-General for Communications Network, Content and Technology
DG GROW	Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
DG INTRA	Directorate-General for International Partnerships
DOSA	Digital open strategic autonomy
DPA	Digital Partnership Agreement
DSR	Digital Silk Road
DTS	Digital Technology Stack
DUV	Deep ultraviolet
ECFR	European Council on Foreign Relations
ECTI	European Tech Champions Initiative
EEAS	European External Action Service
EFSD+	European Fund for Sustainable Development Plus
EIC	European Innovation Council
EMC	Electronics manufacturing cluster
ESA	Economic security attaché
ESDM	Electronic systems design and manufacturing
EUV	Extreme ultraviolet
FDI	Foreign direct investment

FOSS	Free and open source software
GDPR	General Data Protection Regulation
GIZ	<i>Deutsche Gesellschaft für Internationale Zusammenarbeit</i> (German Society for International Cooperation)
IA	Innovation attaché
iCET	US–India Initiative on Critical and Emerging Technology
ICT	Information and communications technology
IDS	International Data Spaces
IMD	International Institute for Management Development
IoT	Internet of Things
IPCEI	Important Projects of Common European Interest
IPEF	Indo-Pacific Economic Framework
IRA	(US) Inflation Reduction Act
IT	Information technology
KPI	Key performance indicator
KYC	(India’s) Know Your Customer
NATO	North Atlantic Treaty Organisation
NIST	(US) National Institute of Standards and Technology
NRCFOSS	(India’s) National Resource Centre for free and open source software
NRRP	(France’s) National Recovery and Resilience Plan
OSA	Open strategic autonomy
PIA	(France’s) Investments for the Future programme
PLI	Production-linked incentive
PS–RP	Promote and Shape – Regulate and Protect
R&D	Research and development
R&D&I	Research, development and innovation
SCO	Shanghai Cooperation Organisation
SCRI	Supply Chain Resilience Initiative
SME	Small and medium-sized enterprise
SPECS	(India’s) Scheme for Promotion of Manufacturing of Electronic Components and Semiconductors
SSDF	(US) Secure Software Development Framework
TTC	Trade and Technology Council
TTDF	Telecom Technology Development Fund
UPI	(India’s) Unified Payments Interface
VTT	(Finland’s) Technical Research Centre
WIC	World Internet Conference
WTO	World Trade Organisation

List of tables

Box 1	Technological sovereignty/autonomy vs. digital sovereignty/autonomy	10
Table 1	EU legislation and instruments to secure DOSA-related interests	33
Table 2	Digital and technology index rankings	43
Table 3	Key digital-enabling technologies from the ASPI Critical Technology Tracker	46
Table 4	Performance of Dutch IA and ESA host countries in digital and technological indices	49
Table 5	Case study of Germany: PS–RP and DTS analysis of digital and technology policies	53
Table 6	Case study of France: PS–RP and DTS analysis of digital and technology policies	59
Table 7	Case study of Finland: PS–RP and DTS analysis of digital and technology policies	65
Table 8	Case study of the United States: PS–RP and DTS analysis of digital and technology policies	70
Table 9	Case study of China: PS–RP and DTS analysis of digital and technology policies	77
Table 10	Case study of India: PS–RP and DTS analysis of digital and technology policies	83

List of figures

Figure 1	Current relations between the EU, US and China	17
Figure 2	Map of the European Union's DPAs and TTCs, as of June 2023	22
Figure 3	Non-exhaustive map of international partnerships in the Indo-Pacific region, where the EU is not engaged	24
Figure 4	Courses of EU action: Promote and Protect, underpinned respectively by Shape and Regulate	32
Figure 5	Dutch Innovation Attachés Network and Economic Security Attachés Network	37
Figure 6	Dutch DOSA focus: five layers of the DTS model	41
Figure 7	Digital Economy and Society Index (DESI), 2022	44
Figure 8	Placement of Dutch IAs and ESAs	47
Figure 9	Quick scan of IA and ESA countries and their relationship to the Netherlands	51
Figure 10	Countries included in in-depth case-study analysis	52
Figure 11	Germany's DTS profile	57
Figure 12	France's DTS profile	63
Figure 13	Finland's DTS profile	68
Figure 14	United States of America's DTS profile	75
Figure 15	China's DTS profile	82
Figure 16	India's DTS profile	89
Figure 17	Promoting–Protecting–Partnering framework, introduced in the European Economic Security Strategy	92

Introduction

Over the past half decade, fundamental geopolitical adjustments and an ongoing rearrangement of the world order have forced governments worldwide to focus more and more on technology and digitalisation. Technological leadership, digital autonomy and economic security are now political *Chefsache* of governments throughout the world, including in Europe. Set against this context, the Dutch government has informed Parliament that it is working on developing implementable measures to act on open strategic autonomy in the digital domain, to be presented during the course of 2023. This report offers a strategic international analysis to inform this initiative.

Three key factors catalysed world governments' focus on technology and digitalisation: (1) the Sino-American competition for technological supremacy that intensified from 2018; (2) the Covid-19 pandemic that started in early 2020; and (3) the Russian war of aggression against Ukraine, initiated in February 2022. These three catalysts triggered a set of fundamental policy shifts in many developed countries, including in Europe. Policymakers appear increasingly concerned with the security and stability of supply chains, 'de-risking', 'friend-shoring', and calls for new and innovative approaches towards industrial policy.

Taken together, these mark a significant paradigm shift away from market-based thinking that prioritises open economies, towards a more geostrategic mindset that is less concerned with strict adherence to neoliberal economic practices. Trade and market efficiency are no longer the sole determinants of action for most policymakers around the globe, including in the Netherlands. The European Economic Security Strategy, launched by European Commission President Ursula von der Leyen in June 2023,¹ moves away from open strategic autonomy² to embrace economic security terminology, reflecting what is becoming the new orthodoxy.

1 European Commission, [An EU approach to enhance economic security](#), 20 June 2023.

2 Open strategic autonomy (OSA) has been the terminology widely used within the European Union, since the beginning of the Covid-19 pandemic, to define the bloc's willingness to have more autonomy in its trade and industrial domains, without belittling the importance of open markets. See Luuk Molthof, Dick Zandee and Giulia Cretti, Clingendael Institute, [Unpacking open strategic autonomy: from concept to practice](#), November 2021.

One key component of OSA revolves around technological and digital themes (see Box 1 below for their interrelationship). Ursula von der Leyen referred to ‘Europe’s digital sovereignty’ in her first State of the Union speech in 2020, and to ‘the importance of investing in our European tech sovereignty’ one year later on the same occasion.³ Indeed, strengthening the EU’s digital sovereignty lies at the centre of the European Commission’s ‘Digital Decade’ agenda.⁴ Digital and technological sovereignty translate into the freedom to choose between different trading partners and solutions – that is, to avoid vulnerabilities and reduce dependencies. In Brussels, and among many policymakers across Europe, these themes are placed in the realm of economic security. Finally, while the Dutch government currently prefers the concept of autonomy (in DOSA), this generally corresponds to technological or digital ‘sovereignty’, as used by other political leaders.

Box 1 Technological sovereignty/autonomy vs. digital sovereignty/autonomy

As national digitalisation efforts accelerate, countries increasingly rely on (hard and soft) infrastructure to provide digital services to their populations. In that regard, **tech sovereignty precedes and enables digital sovereignty**. While most EU member states have achieved significant levels of digitalisation across various indicators, significant dependencies on third countries for technology and software (for example, cloud services dominated by American companies) complicate efforts to secure European tech and digital sovereignty. In short:

→ **Technological sovereignty** refers to a state’s ability to develop and maintain advanced technological capabilities without relying on external sources. More technological sovereignty implies less dependency on technology infrastructure from foreign powers.

→ **Digital sovereignty** refers to a state’s ability to make decisions and assert control over digital activities, being capable of providing (critical) digital services and protecting the rights of citizens in the digital realm. It aims to ensure that a state can exercise authority over digital infrastructure, data flows and critical digital services to protect national security, economic interests and societal values.

3 State of the Union Address by President von der Leyen at the European Parliament Plenary, [2020](#) and [2021](#).

4 European Commission, [A Europe fit for the digital age](#).

Led by the Ministry of Economic Affairs and Climate Policy, the Dutch government is currently preparing guidelines and tangible initiatives to strengthen digital autonomy.⁵ Dutch Minister of Foreign Affairs Wopke Hoekstra, Minister of Economic Affairs and Climate Policy Micky Adriaansens and Minister for Foreign Trade and Development Cooperation Liesje Schreinemacher are leading the Dutch efforts on the whole-of-government approach to DOSA (and economic security). In November 2022, they wrote a joint letter informing the Dutch Parliament about the government's and EU's view and efforts on OSA. The letter highlights the importance of working on three building blocks: strengthening the EU's political-economic foundation; mitigating strategic dependencies; and increasing the EU's capacity to act as a geopolitical bloc. The text underlines the Dutch 'open where possible, protect where necessary' mantra, emphasising the importance of an open economy while safeguarding national security, encouraging economic prosperity and addressing societal challenges. The Dutch government seeks to participate actively in European initiatives that contribute to increasing resilience and pursuing technology leadership. Furthermore, it seeks to work on mechanisms to mitigate strategic dependencies, assess risks, and work with industry and international partners. As the letter consistently stresses, key elements for achieving OSA are its technology and digital components. This report aims to contribute to more clarity on how, with which partners and based on what best practices the Dutch government can direct efforts towards DOSA.

Aiming to contribute to the forthcoming Dutch set of national initiatives for digital autonomy, this report reflects on the geopolitical context that shapes DOSA concerns; showcases the key features of both the European and Dutch approaches to the digital component of digital autonomy; presents a concise overview of the state of play in a selected group of key countries; and offers suggestions for future action.

The report is divided into four main sections. First, it discusses the main contemporary geopolitical trends in the digital and technology domains that inform the questions of why and how the Dutch government, as an EU member state, wishes to act to uphold and strengthen its ability to make autonomous choices and to serve public interests. Second, it presents the core aspects of the European and Dutch approaches to the digital pillar of strategic autonomy.

5 [Kamerbrief over open strategische autonomie](#), 8 November 2022 (in Dutch).

The third section then introduces the key countries that are of relevance to Dutch efforts on DOSA as key partners, rivals, technological leaders or best-practice providers. This two-layered analysis encompasses a quick scan of roughly 15 countries, followed by a more in-depth discussion of the policies and actions of six countries that are particularly significant to the Netherlands. This is accompanied by reflections on the potential for cooperation and/or the need to push back on their actions to secure Dutch and European interests in the tech and digital domains. Building on this, the fourth section outlines actionable steps and offers suggestions for policy proposals and routes for future action.

1 Explaining the turn to DOSA and economic security: geopolitical catalysts and policy shifts

This section presents the most salient shifts in global geopolitics that are emerging from three key catalysts forcing governments worldwide to focus on technology and digitalisation. It then discusses their impact on the ambitions of the Netherlands and the EU with regard to DOSA. By subsequently identifying the international relations coalescing into concrete partnerships and alliances in response to these shifts, this analysis identifies a number of strategic questions that are critical for shaping coherent DOSA guidelines and tangible initiatives.

1.1 Three key catalysts for the ongoing policy shifts

The struggle for technological leadership lies at the heart of ongoing policy shifts, with the worsening of US–China relations over issues of trade and access to critical technologies serving as the primary catalyst. The centrality of these two superpowers to global trade and value chains, the interconnectedness of their economies and China’s increasing assertiveness abroad precipitated the current tensions. Beijing’s significant integration into the global market following its accession to the World Trade Organisation (WTO) in 2001 facilitated China becoming the world’s largest exporting nation by 2009.⁶ In 2011, the United States’ Obama administration launched the ‘Pivot to Asia’ strategy as a first response to curb this Chinese growth and geopolitical rise. Since then, the global political centre of gravity is increasingly shifting towards the Indo-Pacific.⁷

In 2018, what started as a tariff war triggered by the subsequent Trump administration marked the beginning of a turn in how policymakers in developed

6 The Guardian, [China becomes world's biggest exporter](#), 10 June 2010.

7 Brookings Institute, [The American pivot to Asia](#), 21 December 2011.

countries view China – a thinking that quickly spilled over from trade to the realm of technology. Concerns about the security of 5G telecommunication networks (with the United States and some of its allies banning or limiting Huawei infrastructure in their networks) evolved into outright alarm over the perceived strategic threat of a homegrown Chinese chips industry capable of producing advanced semiconductors. Exacerbated further by apprehension towards Chinese data-sharing practices and by Beijing's investments in the use of artificial intelligence (AI) and quantum technologies, Washington's fears now reveal themselves in an increasingly combative economic and foreign policy that readily conflates national and economic security interests. For example, on 7 October 2022, the Biden administration announced export controls on semiconductors and related manufacturing equipment bound for China.⁸ Concurrently, Washington entered into diplomatic discussions with the Dutch and Japanese governments, urging them to adopt complementary measures. This culminated in the announcement of export restrictions on advanced semiconductor manufacturing equipment from both The Hague and Tokyo in the first quarter of 2023.⁹ In a similar move, multiple countries have banned or restricted their public officials from using social media platform TikTok (owned by the Chinese tech company ByteDance) on state-issued devices, invoking data-privacy concerns and security reasons.¹⁰

The global Covid-19 pandemic was a second catalyst for the ongoing policy shifts. Principally, the pandemic demonstrated the importance of digital technologies for governments, businesses and citizens to continue working and interacting remotely. The availability of online platforms and cloud services reduced many of the negative social and economic impacts that lockdowns would otherwise have imposed. However, the pandemic also widened the digital divides within and between countries, revealing the extent to which supply-chain dependencies and disruptions, especially those in technology, could impact the European market. The Chinese 'zero-Covid' policy of mandated, consecutive lockdowns (and its abrupt abandonment in December 2022) highlighted the potential severity of these shocks. The protracted restrictions placed on Chinese

8 US Bureau of Industry and Security, [Public information on export controls imposed on advanced computing and semiconductor manufacturing items to the People's Republic Of China \(PRC\)](#), 7 October 2022.

9 Centre for Strategic and International Studies, [Japan and the Netherlands announce plans for new export controls on semiconductor equipment](#), 10 April 2023.

10 Associated Press, [Here are the countries that have bans on TikTok](#), 4 April 2023.

society and the subsequent wave of Covid infections drastically reduced China's manufacturing output, creating severe disruptions in global supply chains.¹¹ Consequently, European leaders increasingly emphasised the importance of building 'trusted supply chains' and developing strategic initiatives to reduce vulnerabilities over (and dependencies on) goods, namely those coming from China. The underlying goal is to ensure greater stability and security, and to eliminate single points of failure.

The third catalyst for the fundamental policy shifts towards economic security and digital autonomy was Russia's war of aggression in Ukraine, launched in February 2022, which highlighted both the criticality of the digital domain and Europe's acute dependencies in the energy sector. Despite fighting a widespread defensive war on its soil for over a year, Ukraine has continued to function through the application of digital technologies and the expedient migration of data and information technology services to the cloud. These measures allowed the Ukrainian government, and society at large, to maintain a significant level of functionality, even as Ukraine has endured bombardment by Russian military forces. Additionally, digital infrastructure deployment by service providers such as Starlink have facilitated the continuity of communication and data flow between the severely impacted, remote regions of Ukraine and major population centres.¹² On the other hand, Russia invests heavily in digital means to manage global dis/misinformation campaigns and disrupt critical infrastructure.¹³ The successful implementation of these technologies in Ukraine has reinforced the criticality of the digital domain for policymakers both within and outside Europe, resulting in an evolution of Brussels' conception of the digital pillar of OSA. Furthermore, the energy crisis caused by the Russian invasion of Ukraine has forced European countries to reckon with the geopolitical exposure created by overdependency on unreliable trading partners. Free and open trade could no longer be viewed as a singular policy imperative, as the vulnerabilities and dependencies generated by such economic models left national governments with severely curtailed strategic options when responding to Russia's invasion. The difficult process of addressing the energy crisis broadened Europe's conception of international trade and gave rise to further strategic thinking on the composition of supply chains and how they impact national autonomy.

11 *The Guardian*, [Zero-Covid policy is costing China its role as the world's workshop](#), 3 December 2022.

12 Eric Schmidt, *Foreign Affairs*, [Why technology will define the future of geopolitics](#), 28 February 2023.

13 *Time*, [Inside the Kremlin's year of Ukraine propaganda](#), 22 February 2023; and *The Guardian*, [Cyber-attacks have tripled in past year, says Ukraine's cybersecurity agency](#), 19 January 2023.

This policy evolution, precipitated by these three catalysts, has forced policymakers and analysts to acknowledge the necessity for a differentiated approach towards the digital component of open strategic autonomy. There is mounting realisation that a move to a bipolar or multipolar global dynamic will increasingly be defined by competition and rivalries over technology. The European Union and its member states are no exception in this generalised inflection point, and are putting forward their own principles and related policy packages that seek to strengthen Europe's digital and technological sovereignty.

The Netherlands – a key EU member state in the technological and digital realms – has been at the forefront of this debate, calling for a nuanced approach to OSA. Principally, while the goal of maintaining an open and globally competitive single market remains a priority in The Hague, it must be complemented by coordinated action by the EU members states in key areas, such as stricter, EU-wide export controls on critical technologies. However, while such *regulatory* efforts may be welcome, the Dutch remain wary of far-reaching EU-level initiatives, including innovation funds and a European e-identity.

1.2 Strategic questions for the coming decades

The overarching question that should inform Dutch guidelines and tangible initiatives for OSA in the digital domain is: *What manner of digital society do we want for our future?* An answer to this question, in the shape of a 'dot on the horizon', or a joint vision for the future Dutch digital society, is of paramount importance to guide national initiatives in the tech and digital realms. Japan's Society 5.0 provides an interesting example of such a blueprint. Its vision of a human-centred society operated through advanced smart technologies serves as the ambition towards which the Japanese government and civil society are working.¹⁴

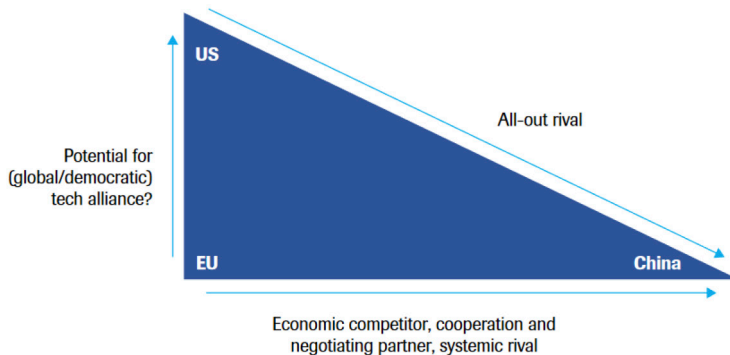
This leading question also shapes ensuing sub-questions. Among them are: (1) how can the Netherlands foster its economic prosperity in the context of DOSA – that is, how to *promote* the Dutch economy to achieve technological leadership?; (2) what trade-offs are at stake and must be managed in order to achieve that vision – that is, what does the Netherlands have to *protect*?;

14 Cabinet Office of the Government of Japan, [Society 5.0: what is Society 5.0?](#)

and (3) with whom can/should the Netherlands cooperate to achieve its strategic goals – that is, how can the Netherlands *shape* the world? Seeking to contribute to answers to these fundamental questions, these keywords – Promote, Shape and Protect – are at the heart of the underlying analysis.

Now, for the first time since the end of the Cold War, national governments are being compelled to reconsider the assumption that the market can operate without intervention and free from geopolitical considerations. In the current paradigm shift, there is a growing emphasis on strategic thinking, heightened awareness of strategic dependencies and vulnerabilities, and the formation of alliances to ensure the existence of viable alternatives. Against this backdrop, the EU wants to emerge as a geopolitical actor next to the United States and China, with its own ideas, strengthened industry and economic model, rather than being in a position of dependence and, in some areas, subalternity. Figure 1, below, illustrates the current relations between the EU, US and China.

Figure 1 Current relations between the EU, US and China



Source: Dekker and Okano-Heijmans (eds), 'Dealing with China on high-tech issues', December 2020.

While seeking to become an independent geopolitical actor in its own right, the EU must continue working closely together with the US, China and rising economies like India to address global challenges such as climate change, without giving up the values upon which the bloc was founded. DOSA embodies a willingness to invest in the ability to defend and uphold European interests instead of being subject to immobilising external pressures. For the EU, this means identifying the precise juncture where autonomy and market openness meet. That may not always be the most economically optimal solution, but the

one that brings lower risks of coercion by reducing dependence on external countries, without excessive and undesirable state intervention in the economy.

Diversification and de-concentration of supply chains to eliminate vulnerabilities and reduce dependencies mark the beginning of a new industrial policy approach. Amid fears of exposure to increasing economic coercion from China, a strategy paper leaked in May 2023 from the European External Action Service highlights that ‘critical dependencies on China leave us vulnerable to weaponisation and coercion in high-tech areas such as renewable energy and communication technologies [...] and raw materials’.¹⁵ The same report points to ‘fierce Chinese competition in domains of unprecedented sensitivity including certain semiconductors, quantum computing, space technologies, Artificial Intelligence, [and] biotechnologies’. In practical terms, European governments and companies are reassessing their supply chains and the extent to which they should relocate them, at least partly, to more reliable countries (so-called ‘friend-shoring’, to build ‘trust supply chains’). The concept of ‘de-risking’ is emerging and replacing the idea of decoupling proposed by the United States during the Covid-19 pandemic, when Europe’s dependency on China for basic goods, such as face masks, was clearly exposed. Now, as US President Joe Biden explained at the May 2023 G7 Summit, ‘we’re not looking to decouple from China; we’re looking to de-risk and diversify our relationship with China’.¹⁶ Given the interdependencies in place, de-risking represents a more moderate and realistic approach to the relationship with China than decoupling.

Accordingly, some multinationals and corporations are considering implementing a ‘China plus one’ approach, to secure an alternative to China within their supply chains.¹⁷ In addition to more traditional partners, such as Japan, South Korea or Singapore, EU governments and companies are also courting countries like India or Vietnam. The extent to which the EU and its member states are able to onboard these countries will also define their ability to achieve their desired strategic autonomy. This new thinking also implies being more careful about knowledge transfer, namely to states or regimes that cannot be trusted. As a consequence, a new type of diplomacy is emerging. European countries, with partners that broadly share the EU’s interests and concerns, are using several

15 EU Observer, [EU looks beyond Russia war to Chinese ‘new world order’](#), 12 May 2023.

16 Reuters, [Biden sees shift in ties with China ‘shortly’](#), 21 May 2023.

17 James Crabtree, *Financial Times*, [The west is in the grip of a decoupling delusion](#), 14 April 2023.

means to influence those ‘non-aligned’ swing states, more recently referred to as the Global South.¹⁸ Such diplomacy aims to persuade them of the virtues and benefits of a rules-based system, as well as ensuring that they understand and adopt similar standards that are underpinned by shared norms and values. In this regard, the war in Ukraine has shown the limitations and challenges that Europe, the United States and their partners face in convincing countries in the Global South to align with them. The approach so far has been to frame the war in Ukraine as a challenge between democracies and autocracies. Yet the limitations of this approach are evident in light of the existing challenges to democracy in some developed countries, as well as the desire to onboard certain developing countries that are not – or not mature – democracies, such as Vietnam. Seen in this regard, the preferred path may be to focus on respect for the rule of law and principles of accountability.¹⁹ Doing so would weaken the rationale behind China’s support of Russia, as Beijing likes to position itself as a proponent of a rules-based system.

Finally, a shift has been occurring from multilateralism to minilateralism.²⁰ Long-existing institutions and forums are losing steam or being abandoned, such as the World Trade Organisation and the Wassenaar Arrangement. In their place, new bilateral and minilateral agreements are emerging to address tech and digital-related themes, from development cooperation to export controls. The next section presents a selection of some of these new formal and informal discussion groups.

1.3 Relevant partnerships

One noticeable feature of the ongoing shifts in global politics is the move of the political centre and (digital) economy to the Indo-Pacific region. This is apparent through the strategic partnerships that both the European Union and the United States have formed. The US has taken the lead in setting up several formal and informal agreements in the region, but the EU has also been active in

18 Some consider the term ‘Global South’ divisive and unhelpful, as it is a label encompassing a very diverse group of nations. However, countries like India now ascribe to and encourage the use of the ‘Global South’ moniker. See: Nikkei, [Modi says he will ‘amplify concerns of Global South’ at G7](#), 19 May 2023.

19 David Miliband, [The survival of the West and the demands of the rest](#), 28 February 2023.

20 Husain Haqqani, *Foreign Policy*, [The Minilateral era](#), 10 January 2023.

creating new spaces for dialogue. Similarly, these changing geopolitical winds have revitalised efforts by leading developing countries to strengthen coalitions and partnerships outside the scope of traditional powers, such as the BRICS group of Brazil, Russia, India, China and South Africa.

Acknowledgement of these shifts informs the structure of this section, which begins by introducing the bilateral forums where the EU has been engaging with other countries, namely in the Indo-Pacific. Second, it offers an overview of key forums where the EU is not participating, but that are still representative of the current policy shifts and include EU partner countries. Third, it presents the forums and initiatives led by China and some of its close partners. Finally, it discusses the ongoing move from multilateralism to minilateralism by addressing the latest developments in the context of the Wassenaar Arrangement, a multilateral export-control regime established in 1996.

1.3.1 The EU in action: Trade and Technology Councils and Digital Partnership Agreements

Since digital autonomy was established as a political priority for the European Commission in 2020, the EU has taken concrete steps to establish new discussion forums dedicated to technology and digital.

The European Union and the United States established a Trade and Technology Council (EU–US TTC) during the EU–US Summit in June 2021.²¹ The goal of this forum is to ‘coordinate approaches to key global technology, economic and trade issues; and to deepen transatlantic trade and economic relations, basing policies on shared democratic values’.²² The EU–US TTC is comprised of ten working groups, from technology standards cooperation, to supply chains, clean tech and export-controls’ cooperation.²³ Although decisions taken within this framework are not legally binding, the initiative *promotes* greater alignment and common understanding on underlying principles.²⁴ One area where there has been most progress is artificial intelligence (AI). The two blocs developed a joint roadmap

21 European Commission, [EU–US Trade and Technology Council](#).

22 European Commission, [EU–US Trade and Technology Council: inaugural joint statement](#), 29 September 2021.

23 European Commission, [EU–US Trade and Technology Council: areas of cooperation](#).

24 European Council on Foreign Relations, [Setting the tone: The value of the EU–US Trade and Technology Council](#), 9 December 2022.

to define common terminologies and taxonomies, as well as to work towards enhanced AI risk management and trustworthy AI.²⁵

Beyond the US, the European Union has focused its attention on building partnerships with countries in the Indo-Pacific. The EU Strategy for Cooperation in the Indo-Pacific states that the region is ‘increasingly becoming strategically important for the EU’ and a ‘key player in shaping the international order and addressing global challenges’.²⁶ Accordingly, the European Union has established so-called Digital Partnership Agreements (DPAs) with Japan, South Korea and Singapore, as well as a Technology and Trade Council with India. The first of such initiatives was the Japan–EU Digital Partnership Agreement in May 2022, followed by the Republic of Korea–EU Digital Partnership Agreement in November 2022 and a Digital Partnership Agreement with Singapore in February 2023.²⁷ The TTC with India was announced in April 2022 and launched in February 2023.²⁸ These partnerships aim to create an environment for the EU to bridge differences and collaborate with partners on the development of standards and research and Development (R&D) initiatives for current and emerging technologies, including digital connectivity, artificial intelligence, semiconductors, 5G and 6G, and quantum computing. These partnerships also aim to enable regulatory cooperation, interchange of capacity-building and skills, as well as to create mutual opportunities for international investment and research partnerships.

As of June 2023, the European Commission is working on promoting the current Digital Dialogue with Canada to a Digital Partnership Agreement. This DPA will likely focus on AI, connectivity, cybersecurity and technology-related R&D initiatives, and aims to foster cooperation on obtaining rare earths and strategic minerals – key resources required for many high-tech products.²⁹ Figure 2 summarises the EU digital agreements currently in place.

25 Euractiv, [EU, US step up AI cooperation amid policy crunchtime](#), 30 January 2023.

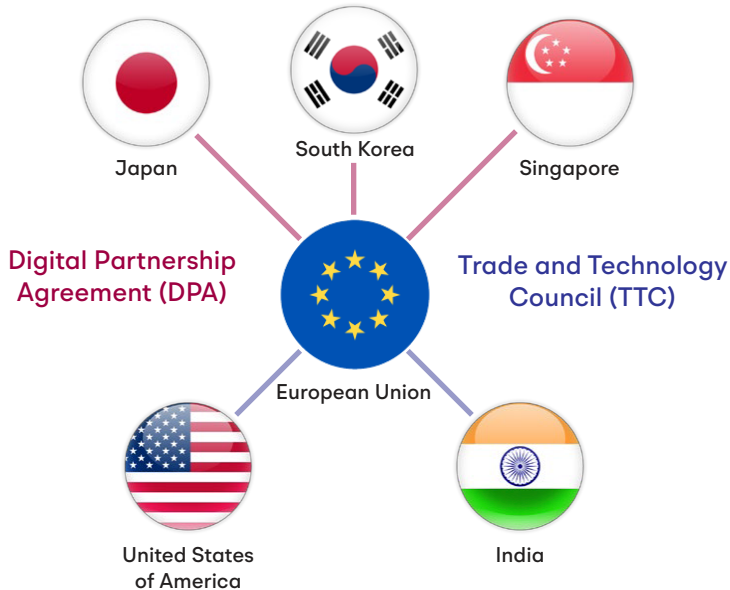
26 European Commission, [Questions and answers: EU Strategy for cooperation in the Indo-Pacific](#), 16 September 2021.

27 European Commission, [Digital partnerships](#).

28 European Commission, [EU-India: new Trade and Technology Council to lead on digital transformation, green technologies and trade](#), 6 February 2023.

29 Euractiv, [Commission updates EU countries on digital diplomacy initiatives](#), 20 April 2023.

Figure 2 Map of the European Union's DPAs and TTCs, as of June 2023



Source: authors' compilation.

Besides the agreements noted above, the EU conducts dedicated cybersecurity dialogues with several partners, including the US, Canada, China, Japan, South Korea, Australia, New Zealand and Ukraine, and with the North Atlantic Treaty Organisation (NATO).

Furthermore, the EU and several EU member states are part of the Group of 7 (G7) and the Group of 20 (G20).³⁰ The 2023 G7 summit, organised by Japan and held in Hiroshima in May 2023, placed economic security – and, albeit largely indirectly, China – at the centre of discussions. The concept of ‘de-risking’ took root and was used instead of ‘decoupling’ in the final G7 communiqué. Without ever explicitly mentioning China, the G7 leaders’ statement on economic resilience highlights de-risking, economic security and anti-coercion.³¹

30 The G7 is an international forum where seven of the largest world economies have a seat to address global issues in the areas of trade, economics and security. The G7 members are the United States, Canada, Germany, France, Italy, Japan, the United Kingdom and the European Union. The G20 is more diverse, and includes – in addition to all G7 participants – Argentina, Australia, Brazil, China, India, Indonesia, Mexico, Russia, Saudi Arabia, South Africa, South Korea and Turkey.

31 *Politico*, [In Hiroshima, Zelenskyy borrows history to fight for the future](#), 21 May 2023.

These were broken down into the following themes: building resilient supply chains; building critical infrastructure; responding to non-market policies and practices; addressing economic coercion; countering harmful practices in the digital sphere; cooperation on international standards-setting; and preventing leakage of critical and emerging technologies.³² Concretely, the group announced the creation of a ‘Coordination Platform on Economic Coercion to increase our collective assessment, preparedness, deterrence and response to economic coercion, and further promote cooperation with partners beyond the G7’.³³ Furthermore, the final G7 communiqué also highlights the importance of collaborative efforts among its members in multistakeholder settings. It specifically underscores the areas of trustworthy AI and ‘the development and adoption of international technical standards’. This emphasis is in line with the push to incorporate ‘governance, public safety and human rights’, as well as interoperability and portability, as key drivers in technological development.

Regarding the G20, whose 2023 summit will be organised by India in September, the host country’s agenda priorities include the track of ‘Technological Transformation and Digital Public Infrastructure’. This track aspires to promote and exchange views of ‘a human-centric approach to technology and increased knowledge-sharing in areas such as digital public infrastructure, financial inclusion, and tech-enabled development in sectors such as agriculture and education’.³⁴ This wording is remarkable, because the ‘human-centric approach’ – that puts people first, and includes a strong focus on ethics, including in data-protection regulations – is precisely the EU’s Digital Decade proposition. It is, however, at odds with some G20 members’ practices, notably China and Russia, making it unpredictable as to what extent this track will make significant developments. The essentially like-minded G7 countries will use the 2023 G20 summit to influence the remaining G20 countries about some of the strategic priorities laid down in the Hiroshima G7 leaders’ communiqué. Those include to ‘support a free and open Indo-Pacific and oppose any unilateral attempts to change the status quo by force or coercion’ and to ‘foster a strong and resilient global economic recovery, maintain financial stability, and promote jobs and sustainable growth’. Behind these goals are ‘international principles and shared values [...] upholding and reinforcing the free and open international order based on the rule of law’.³⁵ The extent to which the

32 White House, [G7 leaders’ statement on economic resilience and economic security](#), 20 May 2023.

33 Politico, [China watcher: G7 unpacked – France wants to bring Germany to Beijing – Xi-stan](#), 23 May 2023.

34 Indian Ministry of Earth Sciences, [Overview of G20](#).

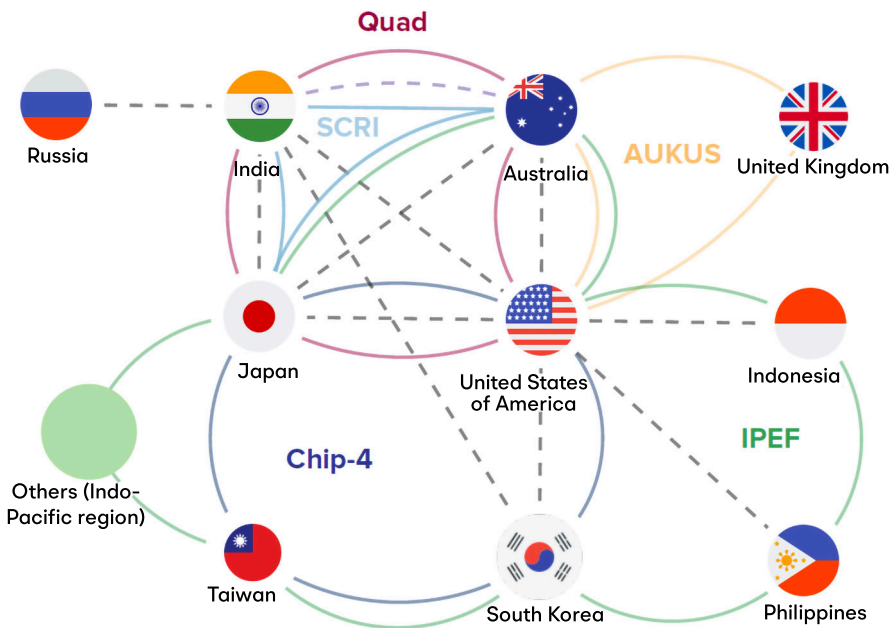
35 White House, [G7 Hiroshima Leaders’ Communiqué](#), 20 May 2023.

G7 members can influence and convince their G20 counterparts – many of whom consider themselves members of the Global South – of the importance of a rules-based world order is of paramount strategic relevance. It will have a lasting impact on the ability of the EU – and the Netherlands – to build lasting partnerships, which will inevitably contribute to DOSA.

1.3.2 Tracking key international forums of relevance to the EU

This subsection highlights important tech and digital forums that involve EU partner or competitor countries. Although the EU is not directly involved in these exchanges, they are still relevant to monitor. They may unveil new trends and ideas in technology and digital, as well as reveal new prospects for collaboration. Figure 3 below summarises some of these partnerships, alliances and bilateral dialogues in place in the region.

Figure 3 Non-exhaustive map of international partnerships in the Indo-Pacific region, where the EU is not engaged



Source: authors' compilation.

Note: Dashed grey lines represent '2+2 Ministerial Dialogues'.

The United States has progressively paid more attention to Asia and the Pacific, beginning with the Obama administration's 'Pivot to Asia' strategy in 2011 as a first response to Chinese growth.³⁶ In late 2017, Donald Trump started using the label 'Indo-Pacific' to refer to the region, rather than the previously more common term 'Asia-Pacific'.³⁷ In 2019, Trump's administration released a vision for a 'free and open Indo-Pacific', along with a set of concrete measures and regional programmes led by the US.³⁸ Under President Biden, the exit from Afghanistan in August 2021 was partly motivated by the United States' need to refocus and allocate more resources to the Indo-Pacific, which was increasingly perceived as being in danger because of the rise of China.³⁹ It is against this backdrop that the US has significantly increased its presence and diplomatic efforts in the Indo-Pacific, trying to build alliances in virtually all fields, from military and energy to infrastructure and cybersecurity.

The Quadrilateral Security Dialogue (also known as the Quad) is a multilateral forum that includes the United States, Australia, India and Japan. The Quad has no less than 20 working groups, many of which focus on non-traditional security, including tech and digital issues. The Quad initiative was initially proposed in 2007 by (then) Japanese Prime Minister Shinzo Abe, to function as a cooperation hub for military purposes. Although initially short-lived, the Quad became active again in 2017, with a focus on collaboration on critical and emerging technologies.⁴⁰ The group met in May 2023 in Hiroshima, on the sidelines of the 2023 G7 Summit. One of the outcomes of that meeting was the announcement of the 'Quad Partnership for Cable Connectivity and Resilience', aimed at securing and supporting under-sea cables serving the Indo-Pacific.⁴¹ Moreover, one should note the rapid improvement of relations between South Korea and Japan since Korean President Yoon Suk Yeol took office. Although talks are still in an early phase, South Korea may join the Quad in the future – if not as a full member, then at least in some of its working groups.⁴²

36 Brookings, [The American pivot to Asia](#), 21 December 2011.

37 Politico, [In Asia, Trump keeps talking about Indo-Pacific](#), 11 July 2017.

38 US Department of State, [A free and open Indo-Pacific: advancing a shared vision](#), 4 November 2019.

39 Bloomberg, [US focus shifting to China from Afghanistan, Blinken says](#), 18 April 2021.

40 Council of Foreign Affairs, [The future of the Quad's technology cooperation hangs in the balance](#), 14 June 2022.

41 Jason Hsu and Charles Mok, [Taiwan's island internet cutoff highlights infrastructure risks](#), 31 May 2023.

42 Nikkei, [Bring South Korea into Quad to cement Japan ties, analysts say](#), 20 March 2023.

In parallel to the Quad, Japan, India and Australia launched the Supply Chain Resilience Initiative (SCRI) in April 2021. After the Covid-19 pandemic shed light on their overdependencies on China, the SCRI was established to find common ground and solutions to overcome supply-chain vulnerabilities.

Another forum for digital and technology cooperation from which the EU and member states are excluded is AUKUS, established in September 2021 by Australia, the United Kingdom and the United States (hence, A–UK–US or AUKUS). Under this security partnership, the three partners will support Australia in acquiring nuclear-powered submarines. Importantly, however, this cooperation spills over to the realm of joint technology development. The group wants to enhance joint capabilities and interoperability, namely on cybersecurity and emerging technologies such as artificial intelligence and quantum technologies.⁴³

In May 2022, Tokyo hosted the launch of a US-led initiative, known as Indo-Pacific Economic Framework (IPEF). A total of 14 countries are engaged, including all four Quad members, South Korea, New Zealand, Fiji and seven countries of the Association of South-East Asian Nations (ASEAN): Brunei; the Philippines; Malaysia; Vietnam; Thailand; Singapore; and Indonesia.⁴⁴ Some of the key themes on IPEF's agenda are supply-chain security, clean energy, decarbonisation and infrastructure.⁴⁵ In May 2023, the group met in Detroit in the US and agreed for the first time on concrete measures to address microchip supply-chain disruptions and to address dependencies on critical materials from China. The mechanisms outlined include information sharing about potential supply-chain risks and cooperation to address shortages.⁴⁶

Moreover, the United States has taken steps to establish a platform for key actors in the semiconductor industry to coordinate their policies. This so-called Chip 4 Alliance includes the governments of Japan, South Korea, Taiwan and the US, as well as key companies such as TSMC and Samsung. By engaging instrumental countries along the semiconductor value chain, the US hopes not only to increase its technological lead over China in this critical technology, but also to convince its

43 US Department of Defense, [AUKUS: the trilateral security partnership between Australia, UK and US](#).

44 Japan Ministry of Economy, Trade and Industry, [Basic economic knowledge: the Indo-Pacific Economic Framework \(IPEF\), a new framework for economic collaboration](#), 7 November 2022.

45 Office of the United States Trade Representative, [Indo-Pacific Economic Framework for Prosperity \(IPEF\)](#).

46 Nikkei, [IPEF nations agree to strengthen supply chains at Detroit meeting](#), 28 May 2023.

counterparts of the strategic value in forestalling the growth of the Chinese chips sector. However, Japan and South Korea are not yet fully on board because of concerns about China's perception of their participation in this dialogue. China is the most important economic partner for both Japan and South Korea, and they fear the reaction of China if they join forces with Taiwan, given the latent tensions between the island and mainland China.⁴⁷ In May 2023, Japanese Prime Minister Fumio Kishida held talks with senior executives of key players from the industry, including Taiwan's TSMC, South Korea's Samsung, and Intel, Micron and IBM from the United States, and announced new investments to be made in Japan in this sector.⁴⁸

Furthermore, bilateral '2+2 Ministerial Dialogues' are taking place between several countries in the Indo-Pacific region. These dialogues, comprising the ministries of foreign affairs and the ministries of defence or economy of two partnering countries, often include discussions on technology and digital.⁴⁹ In July 2022, the US and Japan held their first 'Economic 2+2' meeting. At the heart of this meeting were economic security and resilience. Given the increasing importance attached to the topic of economic security, this format is likely to be replicated by other bilateral relationships over the coming years.

1.3.3 The end of a unipolar world: China's push to great power status

China has engaged in multiple initiatives to increase its influence around the globe. The most successful is the so-called Belt and Road Initiative (BRI) – and especially relevant for the purpose of this report its digital pillar, the Digital Silk Road (DSR). The BRI is a large-scale infrastructure and investment initiative launched in 2013 by China's President Xi.⁵⁰ Its ambitious goal is to build a network of infrastructure in areas such as transportation, energy and telecommunications to connect East Asia with Europe, as well as Africa, Oceania and Latin America. China's push for the DSR is driven by a desire to globalise its technology and standards: combining an internal push to develop Chinese technologies in areas like 5G, AI and the internet of things (IoT) with an agenda to extend

47 *Financial Times*, [US struggles to mobilise its East Asian 'Chip 4' alliance](#), 13 September 2023.

48 *Japan Times*, [Micron reveals ¥500 billion Japan chip plan after PM meets execs](#), 18 May 2023.

49 US Department of State, [Fourth annual US–India 2+2 Ministerial Dialogue](#), 11 April 2022; US Embassy and consulates in Japan, [Joint Statement of the Security Consultative Committee \(2+2\)](#), 11 January 2023; and Australia Ministry for Foreign Affairs, [Tenth Japan–Australia 2+2 Foreign and Defence Ministerial Consultations](#), 9 December 2022.

50 Council on Foreign Affairs, [China's massive Belt and Road Initiative](#), 2 February 2023.

Chinese influence abroad, by enhancing interoperability with networks abroad. Importantly, the DSR was facilitated at least in part by China's 'Made in China 2025' industrial strategy. Launched in 2015 to 'modernise and reform its domestic manufacturing sector' by making it more high-value and innovation-driven, this is one of the clearest hallmarks yet of China's push for technological leadership.⁵¹ Beijing's 'China Standards 2035 Strategy' of 2022, which aims for China to go global with its technical standards, is a more recent step on this path.

The Shanghai Cooperation Organisation (SCO) is an intergovernmental organisation founded in 2001 and formed by China, India, Kazakhstan, Kyrgyzstan, Pakistan, Russia, Tajikistan and Uzbekistan. The SCO was originally focused on security, terrorism and extremism issues, but its scope has extended to regional development and economic cooperation.⁵² India, which joined the organisation in 2017, is responsible for bringing two new cooperation pillars to the organisation: Start-ups and Innovation; and Science and Technology.⁵³ India will host the 2023 SCO Summit, and one of its focuses will be connectivity. However, the SCO's output is not particularly promising. Border tensions between some of its members – namely China, India and Pakistan – restrain the effectiveness of the organisation. In early May 2023, the SCO foreign ministers' meeting took place, with the Indian and Pakistani ministries of foreign affairs blaming each other for the tensions in Kashmir and current relations between their countries.⁵⁴ In May 2023, the Indian authorities surprisingly announced that the 2023 SCO Summit, scheduled for July, would be held in virtual format, and not in person as originally expected.⁵⁵

A forum where China tries to extend its sphere of influence is BRICS, the group consisting of Brazil, Russia, India, China and South Africa. Together, BRICS group represents approximately 42 per cent of the world's population and more than 25 per cent of global GDP.⁵⁶ While the group has foundered over the last four years, the return to power of Brazilian President Lula da Silva in October 2022 may reignite activity. Themes such as connectivity, raw materials and

51 Brigitte Dekker, Maaïke Okano-Heijmans and Eric Sihi Zhang, [Unpacking China's Digital Silk Road](#), July 2020.

52 United Nations Political and Peacebuilding Affairs, [Shanghai Cooperation Organisation](#).

53 India in SCO, [India and SCO](#).

54 Reuters, [India and Pakistan trade blame for frosty ties after SCO meeting](#), 5 May 2023.

55 Reuters, [India to host SCO summit in virtual format in July](#), 31 May 2023.

56 United Nations Conference on Trade and Development, [BRICS Investment Report](#), 2022.

emerging technologies will have growing relevance in this forum. The Brazilian president has used the first quarter of his term in office to advocate publicly for a realignment in geopolitics and the need to create an alternative economic system to that dominated by US institutions. In April 2023, during a visit to a Huawei R&D centre in Shanghai, Lula da Silva made clear that he has no ‘security concerns’, nor ‘prejudices’, in relation to Chinese technology, telecommunications or China’s semiconductor industry.⁵⁷ China and Brazil signed 15 agreements, five of which addressed technology and digitalisation. These include the joint development of a sixth China–Brazil Earth Resources Satellite (CBERS-6), to monitor the Amazon and collect climate-related data; and cooperation agreements in research, development and innovation (R&D&I), information technologies, telecommunications (including 5G networks), digital economy and space. Brazil’s turn towards China – and with that, Chinese principles and standards – shows that European countries need to act globally if they wish to uphold not only their own digital autonomy at home, but also a secure world in which European digital standards and rights inspire others.

1.3.4 The end of multilateralism... Long live unilateralism?

One practical consequence of deteriorating unipolarity is the fading importance of multilateral organisations and agreements created by, or in the interests of, the United States. An example of this phenomenon, with particular relevance to the quest for digital autonomy, can be seen in the growing irrelevance of the Wassenaar Arrangement.⁵⁸ The effectiveness and usefulness of the agreement were severely impacted by the Russian war of aggression against Ukraine, which made communication between Russia and the remaining participant countries impossible, and the United States’ unilateral imposition of semiconductor export controls on China on 7 October 2022. In 2019, the Trump administration had already convinced the Netherlands’ government not to allow Dutch high-end technology company ASML to export its extreme ultraviolet (EUV) lithography machines, which are vital for manufacturing the most advanced chips in the world at a very large scale.⁵⁹ This decision not only hampers China’s ability to produce advanced chips for military uses, thus impacting regional (and national) security, but will also help the US to achieve its stated goal of maintaining

57 Reuters, [Lula courts Chinese tech for Brazil, brushes off ‘prejudices’](#), 14 April 2023.

58 The Wassenaar Arrangement is a multilateral export-control regime established in 1996 with 42 participating states, aiming at facilitating knowledge-sharing and transparency regarding the export of conventional arms and dual-use goods and technologies.

59 CNN, [US orders Nvidia and AMD to stop selling AI chips to China](#), 1 September 2022.

'as large of a [technological] lead as possible'.⁶⁰ The restrictions imposed include control over the export of advanced chips, chip design software and chip manufacturing equipment. The regulations also forbid US citizens, residents and Green Card holders from supporting the development or production of certain semiconductor products without a licence. Notably, in October 2022, some non-US companies, including Samsung and TSMC, received a general one-year licence to continue operating in China in order for international supply chains to continue to function.⁶¹ Over the months after these unilateral decisions were announced, the United States dedicated extensive diplomatic efforts to convince other key players in the industry, namely Japan and the Netherlands. These two countries eventually announced, in early 2023, that they would also impose restrictions in the sector.⁶² Since then, diplomats have been looking for new multilateral approaches to replace the Wassenaar Arrangement setting, an example of a long-standing institution that has progressively diminished in importance over time.

60 White House, [Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit](#), 16 September 2022.

61 Center for Strategic and International Studies, [A seismic shift: the new US semiconductor export controls and the implications for US firms, allies, and the innovation ecosystem](#), 14 November 2022; and Nikkei, [Samsung and SK Hynix face China dilemma from US export controls](#), 25 October 2022. As of June 2023, it is unknown whether these licences will be renewed. Also see US Department of Commerce, Bureau of Industry and Security, [Commerce implements new export controls on advanced computing and semiconductor manufacturing items to the People's Republic of China \(PRC\)](#), 7 October 2022; and US Federal Register, [Implementation of additional export controls: certain advanced computing and semiconductor manufacturing items; supercomputer and semiconductor end use; entity list modification](#), 13 October 2022.

62 *Financial Times*, [Japan to restrict semiconductor equipment exports as China chip war intensifies](#), 31 March 2023.

2 The European and Dutch approaches to the digital dimension of strategic autonomy

2.1 Europe's digital decade?⁶³

While the concept may change from one year to the next, or vary by country, the core concepts underpinning digital autonomy have moved up the agenda of EU institutions and of a growing number of European capitals in recent years. As noted above, European Commission President Ursula von der Leyen used her State of the Union speeches to highlight digital sovereignty for the first time in 2020, and technological sovereignty in 2021.⁶⁴ Germany made digital sovereignty one of the four priorities of its EU Presidency in the latter half of 2020. And in February 2021, President of the Council of the European Union Charles Michel stated that there is 'no strategic autonomy without digital sovereignty'.⁶⁵

The European Commission has acted upon this commitment, proposing legislation and instruments in response to the challenges that have arisen in the technology and digital realms. The 2016 General Data Protection Regulation (GDPR) is just one well-known example of this. The Artificial Intelligence Act (AI Act) that is now under negotiation and the Critical Raw Materials Act (CRM Act), which was announced by the Commission in March 2023, are other examples that show the effort being made to address strategic elements of DOSA.

63 See Brigitte Dekker and Maaike Okano-Heijmans, Clingendael Institute, [Europe's digital decade? Navigating the global battle for digital supremacy](#), October 2020.

64 State of the Union Address by President von der Leyen at the European Parliament Plenary, [2020](#) and [2021](#).

65 European Council, [Digital sovereignty is central to European strategic autonomy – speech by President Charles Michel at 'Masters of digital 2021' online event](#), 3 February 2021.

Such policies and actions of the EU and EU member states may be mapped against two courses of action: Promote; and Protect. The Promote element intends to strengthen and steer economies and societies through trade, investments and innovation, and to make use of our capabilities in equipment, personnel, information and capital. The Protect element aims at addressing dependencies and vulnerabilities in order to improve resilience. Both elements are underpinned by ‘Shape and Regulate’ components. Shape primarily contributes to Promote, as this element encompasses the diplomatic and regulatory efforts aimed at exerting a constructive and positive influence abroad. Regulate mainly contributes to Protect, by providing the legal foundations to help accomplish the goals defined to safeguard and uphold European interests. Together, these four elements constitute the PS–RP framework (Promote and Shape – Regulate and Protect), proposed by the authors to bring clarity to this analysis. Figure 4 summarises the PS–RP building blocks.

Figure 4 Courses of EU action: Promote and Protect, underpinned respectively by Shape and Regulate



Source: adapted from Maaïke Okano-Heijmans, ‘Open strategic autonomy: the digital dimension’, Clingendael, 23 December 2022.

Only when acting on each of these components can the EU and its member states appropriately secure European interests involved with DOSA. Table 1 below presents a summary of the legislation that has been, and still is being, implemented over recent years by the EU in the Promote and Protect spheres of action.

Table 1 EU legislation and instruments to secure DOSA-related interests

DTS Layers ⁶⁶	Promote and Shape	Regulate and Protect
Applications and Services	<ul style="list-style-type: none"> Artificial Intelligence Act^{SR} International Data Spaces (IDS) Blockchain Strategy Coordinated Plan on Artificial Intelligence (AI) 	<ul style="list-style-type: none"> Cyber Resilience Act^{SR} Digital Markets Act^{SR} Digital Services Act^{SR} AI export controls Foreign direct investment screening Artificial Intelligence Act^{SR}
Data	<ul style="list-style-type: none"> Data Governance Act^{SR} 	<ul style="list-style-type: none"> General Data Protection Regulation^{SR} Data Act^{SR}
Soft Infra-structure	<ul style="list-style-type: none"> Data Governance Act^{SR} Mobile telecom standards (6G) 	<ul style="list-style-type: none"> Cyber Resilience Act^{SR} Network and Information Systems 2.0 Directive^{SR} Cloud Act^{SR}
Hard Infra-structure	<ul style="list-style-type: none"> Digital for Development (D4D) Global Gateway Quantum technology European Chips Act^{SR} European Battery Alliance Net-Zero Industry Act^{SR} Green Deal Industrial Plan^{SR} 	<ul style="list-style-type: none"> Cyber Resilience Act^{SR} Network and Information Systems 2.0 Directive^{SR} Export controls Foreign direct investment screening Green Deal Industrial Plan^{SR}
Raw Materials	<ul style="list-style-type: none"> European Green Deal^{SR} Critical Raw Materials Act^{SR} 	<ul style="list-style-type: none"> Outbound Investment Screening Cybersecurity Act^{SR} Economic coercion tool Interdependence inventory Resources Strategy Critical Raw Materials Act^{SR} European Green Deal^{SR}

Source: authors' compilation.

Note: SR refers to Shape and Regulate initiatives.

66 DTS refers to Digital Technology Stack. This framework, and its five layers as presented in this table (Applications and Services; Data; Soft Infrastructure; Hard Infrastructure; and Raw Materials), will be elaborated upon in section 3.1 and Figure 6.

2.2 The Dutch turn to DOSA

The Netherlands was pulled into the US–China tech rivalry when the debate about the risks of using Huawei’s equipment for building a 5G network was initiated in 2019. The Dutch government has since then shown itself to be a trustworthy US ally, over time acting in sync with the US on key issues, while at the same time investing in its own – and in Europe’s – technological and digital strengths.

The first debate in the Netherlands in relation to China revolved around Chinese foreign direct investment (FDI). The theme has been subject to public scrutiny at least since 2012, when a handful of Dutch political parties questioned the Dutch government about what measures were being taken in relation to *protecting* the telecommunications sector.⁶⁷ In 2017, Chinese FDI in the Netherlands peaked, reaching a total of about 3.4 billion euros. This value was mostly because of the acquisition of NXP Standard Products by JAC Capital, estimated at 2.75 billion euros.⁶⁸ NXP operates in the semiconductors industry, which is of special relevance to meet DOSA goals. In June 2023, the so-called ‘Vifo Act’ introduced a review of investments, mergers and acquisition activities that could pose a risk to national security (in Dutch: *Veiligheidstoets investeringen, fusies en overnames*, known as *Wet Vifo*). The law is based on an EU regulation of 2019 that seeks to establish ‘a framework for the screening of FDI into the Union’,⁶⁹ and applies to providers considered vital and companies dealing with sensitive technology.⁷⁰

A second heated discussion was related to the Netherlands’ national 5G network. In 2019, citing national security concerns, the US Commerce Department had placed Huawei on its so-called ‘Entity List’, which effectively put the

67 Frans-Paul van der Putten, Clingendael Institute, [Chinese direct investment in the Netherlands: patterns, reception and political significance](#), December 2017.

68 NXP Semiconductors, [NXP announces completion of standard products business divestiture](#), 7 February 2017; and Rhodium Group and MERICS, [Chinese FDI in Europe: 2021 update](#), 27 April 2022.

69 [Official Journal of the European Union, Regulation \(EU\) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union](#), 19 March 2019.

70 Government of the Netherlands, [Besluit Veiligheidstoets voor investeringen, fusies en overnames naar Raad van State](#), 23 December 2022 (in Dutch).

company out of the United States' 5G network.⁷¹ In 2020, the Dutch government approved the Telecommunications Security and Integrity Decree. This legislation provides the legal basis for the Dutch government to require telecom providers to use only products and services of trusted parties in their core networks.⁷² The following year, in 2021, telecom providers operating in the Netherlands were informed by the Dutch government that they had to phase out and replace their Huawei equipment installed at the core network.⁷³

A third focal point of turmoil stems from the role of the Dutch leading semiconductor-manufacturing equipment company ASML. Europe's most valuable tech company, ASML has a global monopoly on the most advanced photolithography machines, based on extreme ultraviolet (EUV) technology, and also has a key role in advanced deep ultraviolet (DUV) machines. In March 2023, the Dutch government announced new export-control measures on advanced semiconductor manufacturing equipment. The new measures target EUV and some DUV machines (including advanced mechanical engineering technologies), which will affect ASML's business in China.⁷⁴ This move results from extensive consultations and negotiations between the US administration and its Dutch counterpart. Japan, which is home to two other DUV equipment producers, has also been under huge pressure. Also in March 2023, Tokyo announced plans to include 23 types of semiconductor-manufacturing equipment in a list of products that cannot be exported to China. This is the result of a trilateral dialogue involving the United States, the Netherlands and Japan.⁷⁵

The Netherlands' involvement in these debates over critical digital technologies – together with the evolution of the strategic autonomy concept within the EU – contributed significantly to the current interest in DOSA. Each of these cases ultimately stemmed from China's rise as a global superpower, and each has

71 CNBC, [Huawei says US blacklisting led to \\$12 billion revenue shortfall in 2019 as profit growth slowed](#), 31 March 2020.

72 Government of the Netherlands, [Maatregelen bescherming telecomnetwerken en 5G](#), 1 July 2019 (in Dutch); and Government of the Netherlands, [Decision on security and integrity telecommunication \[Besluit veiligheid en integriteit telecommunicatie\]](#), 1 March 2020 (in Dutch).

73 [Het Financieele Dagblad](#), [Huawei-ban jaagt telecombedrijven op kosten](#), 28 June 2021 (in Dutch).

74 Government of the Netherlands, [Letter to Parliament on additional export control measures concerning advanced semiconductor manufacturing equipment](#), 10 March 2023.

75 [Financial Times](#), [Netherlands and Japan join US in restricting chip exports to China](#), 27 January 2023.

required careful consideration of Dutch exposure to strategic risks within the context of a shifting geopolitical landscape.

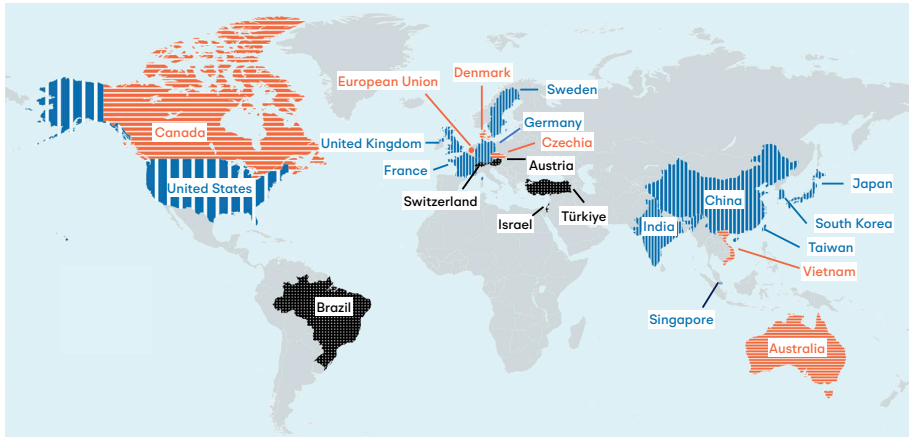
2.2.1 Promoting and Protecting DOSA interests in the world: diplomatic networks

The Dutch government has long understood the importance of cooperation with key partners on digital and technology. The establishment in 1953 of an Innovation Attachés (IA) network, part of the Netherlands' Ministry of Economic Affairs and Climate Policy, illustrates the Dutch desire to invest in collaborating and exchanging information with key players on pivotal issues of interest. Even if the daily operations of these attachés were long guided by economic interests – that is, business promotion – rather than strategic interests such as the quest for DOSA, the network can today be framed on the Promote line of action. Among the main goals of the IA network are to identify trends in innovation and R&D and to promote partnerships with leading players abroad. In recent years, cybersecurity and cyber dialogues have come to feature large on the agenda of these attachés in certain countries, including in Singapore and Beijing.

Most recently, since 2023, with mounting awareness and rising concerns regarding economic security, the Netherlands is also introducing Economic Security Attachés (ESAs) in key countries worldwide. The Dutch definition of economic security revolves around addressing the strategic challenge of responding to issues such as: (1) resilience against the use and misuse of economic activities for geopolitical interests, which may pose a risk to national security; and (2) the integrity of knowledge-intensive sectors and businesses operating with international parties or governments.⁷⁶ Principally, these activities include (digital) espionage, unwanted interference from foreign governments, the export of dual-use goods and applications, as well as foreign investments, acquisitions and mergers. Economic security typically considers, among other things, export controls, sensitive technologies, critical raw materials, investment screening and cybersecurity. The presence of an ESA in a country indicates its criticality for one or more of these focus areas, including countries like China, which is the subject of multiple economic security measures. Figure 5 below presents the locations where Dutch IAs and ESAs are based.

76 Government of the Netherlands, [Wat is economische veiligheid?](#) (in Dutch).

Figure 5 Dutch Innovation Attachés Network and Economic Security Attachés Network



Note: In black: countries with Innovation Attachés only; in orange: countries with Economic Security Attachés only; in blue: countries with both Innovation Attachés and Economic Security Attachés.

Source: authors' compilation.

As explained earlier, the IA network may be regarded as an asset on the Promote side of Dutch technology policy, while the ESA network focuses on the Protect side. Together, they play an important role in the Netherlands' approach to DOSA, ensuring the continuous acquisition of information, maintaining up-to-date knowledge on developments and policies in key countries, and acting on opportunities to cooperate or to contest where necessary.

In addition to IAs and ESAs, the Netherlands also posts Cyber Attachés and Education and Science Attachés (who also address the topic of knowledge security⁷⁷) at certain embassies. The Netherlands is especially active in Cybersecurity Dialogues with other states, including with the United Kingdom, South Africa, India, Indonesia and the United States. The topics discussed within these bilateral talks range from cyber diplomacy, cyber resiliency and incident response, to cyber capacity-building, internet governance, critical and emerging technologies and supply-chain security, as well as cooperation against cyber crime. Cyber Attachés and Education and Science Attachés also contribute to *promoting* and *protecting* DOSA interests, and cooperate closely with the IAs

77 *Loket Kennisveiligheid* in Dutch. See: Government of the Netherlands, [Loket Kennisveiligheid](#) (in Dutch).

and ESAs. They are based in a selection of countries that overlaps with the other networks and therefore are not considered in further detail in this report.

2.3 Concluding remarks

Against the backdrop of the geopolitical catalysts and policy shifts described in section 1, European Commission President Ursula von der Leyen promised to lead a 'geopolitical Commission' upon taking office in 2019.⁷⁸ Accordingly, the European Commission started focusing on digital and technological sovereignty and on how to address those matters. It implies a comprehensive policy roadmap that acts upon both the Promote and Protect agendas, which the Commission has been doing via the introduction of legislation and the creation of tailored programmes such as Global Gateway and its Economic Security agenda. This new thinking has developed in parallel with growing investments in these fields in various EU national capitals. While the EU is often the most forward-leaning, the Netherlands has been a front-runner among EU member states. Acting on their own priorities and interests, EU member states are moving at different speeds on the many sub-sets – whether export controls, digital government, quantum technologies, Digital for Development, connectivity or otherwise.

The centrality of the Netherlands in some critical technologies, such as semiconductors and quantum computing, pushes the country to the forefront of the European debate about what is domestically known as DOSA. However, the big policy shift that the Netherlands is going through also requires continuously paying attention to what partners, competitors and rivals are doing. The next section will shed some light on where the Netherlands should look in order to carry out further its DOSA implementation.

78 Politico, [Meet von der Leyen's 'geopolitical Commission'](#), 4 December 2019.

3 Partners, rivals and best-practice countries

The Dutch national action plan for securing OSA in the digital domain can draw inspiration from – and must be related to – the policies and initiatives of key countries at the forefront of technological development and digital strategy. To this end, this section presents six case studies of significant EU member states and third countries: Finland; France; Germany; the United States; China; and India. This analysis uses both the Promote and Shape – Regulate and Protect (PS–RP) framework discussed in section 1 and a simplified version of the Digital Technology Stack (DTS)⁷⁹ model to provide insights into how various national governments seek to secure technological leadership and autonomy in the digital domain. Together with the foregoing assessment of current geopolitical trends, this section provides the basis for the policy recommendations outlined in section 4 of this report.

3.1 The Digital Technology Stack

While the PS–RP framework provides a compelling basis for categorising courses of action aimed at achieving DOSA, it lacks the analytical capacity needed for a comprehensive comparative analysis of national strategies. Specifically, while it can broadly illustrate the proportion of ‘defensive’, ‘offensive’ and ‘rule-setting’ measures that comprise an actor’s OSA approach in the digital domain, it cannot identify to *which areas* of the digital and technology landscape these measures pertain. For example, how does technological leadership (or lack thereof) in semiconductors and cloud computing impact Dutch and European DOSA? How much should this justify the spending of taxpayers’ money to maintain or enhance technological strength? And how do stricter export controls on semiconductors influence Dutch DOSA, considering the possibility of counter-measures by countries on which the Netherlands relies for critical raw materials that are needed for batteries, chips and other key enabling technologies?

79 Maaik Okano-Heijmans, Clingendael Institute, [Open strategic autonomy: the digital dimension](#), 23 December 2022.

To achieve the specificity needed to answer these questions, this report utilises a modified version of the DTS model.⁸⁰

Originally used by engineers to conceptualise layers of technology in any specific product or service, the scope and usage of Stacks across a variety of industries have expanded in the literature, and more recently made its way into policymaking circles. The Stack may contain a variety of layers, from physical hardware to business processes, and can be leveraged to analyse complex systems and physical goods beyond the realm of software. The DTS model takes this framework a step further, expanding the Stack structure beyond the scope of a single product to conceptualise digital technologies collectively as layers of technological and non-technological components.⁸¹ By applying this generalised Stack model on a national scale, the DTS transforms from a framework for analysing digital systems to a tool for conducting strategic analyses of individual countries' capabilities in the digital domain. Put another way, the model conceptualises a 'national DTS' that represents a combination of technological and non-technological layers constituting a country's digital capacity. By combining the PS–RP framework with the DTS model, this report can compare national investments in the PS–RP courses of action, while also mapping those investments to specific Stack layers, thus illustrating the focal points of different countries' DOSA strategies.

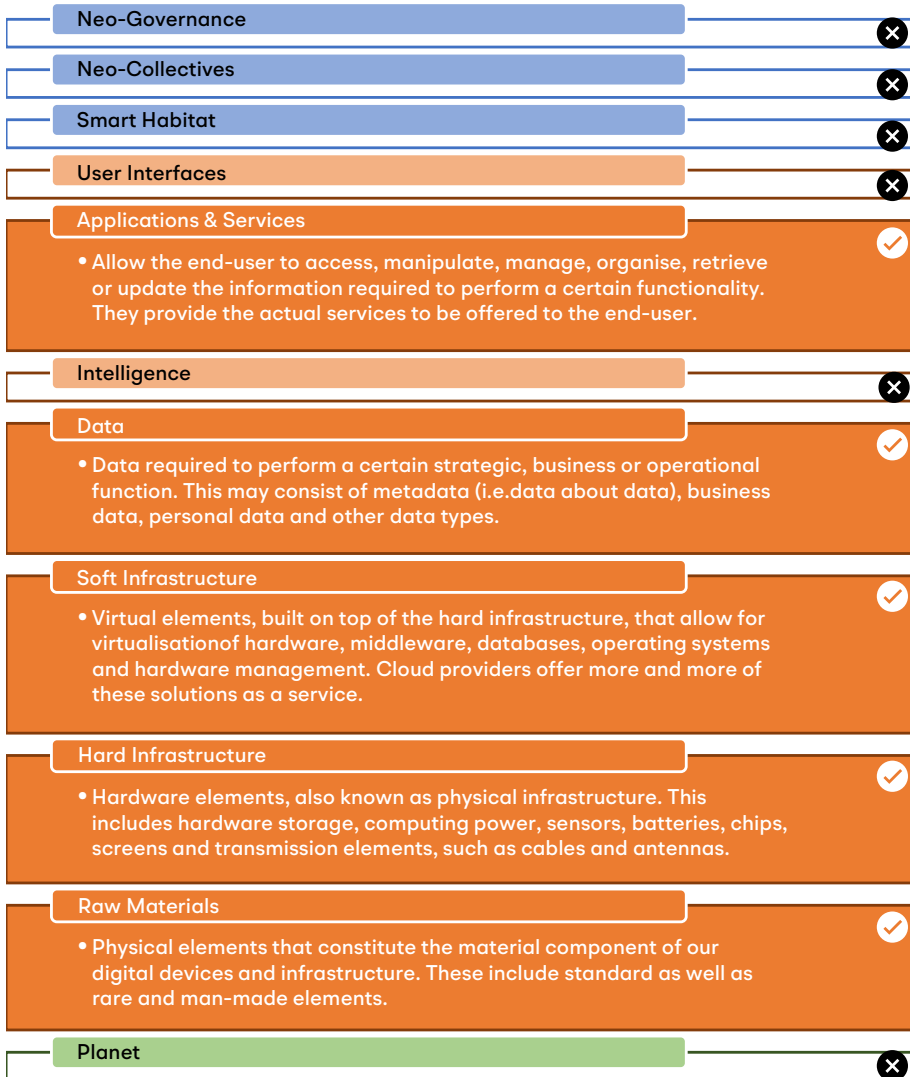
For the purposes of this report and its recommendations for a Dutch DOSA approach, the following case studies utilise a simplified version of the DTS comprised of the Raw Materials, Hard Infrastructure, Soft Infrastructure, Data and Applications & Services layers, as shown in Figure 6. These five layers represent the most salient areas of investment to develop a national DOSA approach. While the top three layers concerned with digital society and culture shape how digital technologies function in a national context, they have limited impact on strategic autonomy. Furthermore, the PS–RP analysis captures elements of governance through the 'Shape and Regulate' course of action. Similarly, while digital technologies rely upon the User Interface and Intelligence

80 The DTS builds on the concept of the 'Technology Stack' – alternatively referred to as a 'Solution Stack' or 'Software Stack' – frequently used by software developers to build systems, platforms and applications. A Technology Stack conceptualises the various building blocks of these digital goods, such as programming languages, operating systems, user interfaces and data storage, as individual layers. When stacked together, they combine to create a complete digital product. Critically, each layer serves a vital function and each must be present for the Stack to function.

81 Sebastiaan Crul, Freedom Lab, [An introduction to the Stack](#), 29 March 2022.

layers, their applicability to building a DOSA approach appears relatively insignificant compared to the other components in this section of the DTS.

Figure 6 Dutch DOSA focus: five layers of the DTS model



Note: ✓: layer within scope of this report; ✗: layer outside scope of this report but within original DTS model.

Source: authors' compilation, adapted from Maaïke Okano-Heijmans, 'Open strategic autonomy: the digital dimension', Clingendael, 23 December 2022.

3.2 Quick scan: partners and rivals in an evolving geopolitical landscape

To isolate six countries for the case-study analysis, this report performs a ‘quick scan’ exercise to identify various partner, competitor and rival countries at the forefront of technological and digital leadership. The following section outlines the quick scan methodology and demonstrates why Finland, France, Germany, the United States, China and India should be considered when formulating the Dutch approach to DOSA.

Although the PS–RP framework and DTS model provide the analytical tools to conduct the case-study analysis, a critical question remains: which countries should the Netherlands look to when formulating its DOSA guidelines and tangible initiatives? Answering this question requires an understanding of:

- 1) Which countries the Netherlands can – or would do well to – partner with, based on shared interests and concerns;
- 2) Which countries the Netherlands rivals and competes with in the digital domain;
- 3) Which countries possess the potential to influence current geopolitical trends at either the EU or global levels; and
- 4) Which countries the Netherlands views as frontrunners in technological development and leaders in the digital domain.

While the first three considerations can be determined through an understanding of Dutch bilateral relations, the Netherlands’ digital profile and the current state of affairs in international relations, the fourth consideration requires additional analysis of digital and technological indicators. To this end, leveraging international rankings of the national capabilities in the digital and technological spheres can identify so-called ‘best-practice countries’ in these areas.

3.2.1 Digital and technological leaders

For the purposes of this quick scan, countries that receive high scores in one or more of these indices can be considered ‘leaders’. While not all measures of digital and technological leadership in these rankings map directly to the DOSA debate (for example, digital skills education), a high composite score demonstrates national investments in a range of digital focus areas. For example, the European Union’s Digital Economy and Society Index (DESI), the International Institute for Management Development’s (IMD) World Digital Competitiveness Ranking and the Cisco Digital Readiness Index represent adequate indicators of digital leadership. Similarly, the European Council on Foreign Relations’ (ECFR) European Sovereignty Index provides an indicator of technology leadership. Table 2, below, includes a short description of each index and lists the top 15 countries from each for the most recently available year.

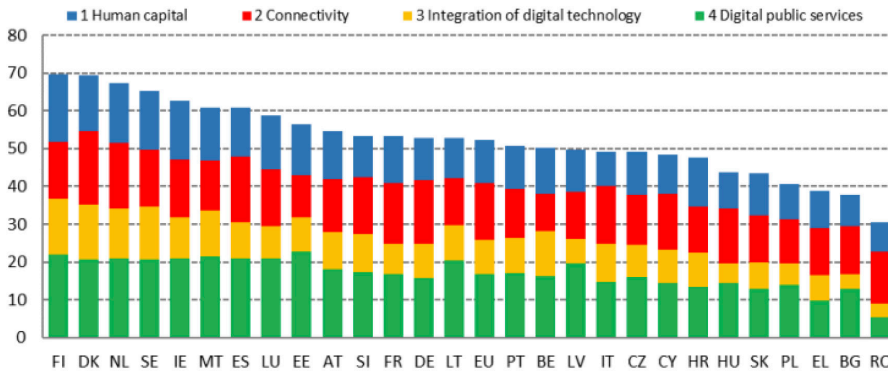
Table 2 Digital and technology index rankings

Rank	Digital			Technology
	Digital Economy and Society Index (2022) ¹	IMD World Digital Competitiveness Ranking (2022) ²	Cisco Digital Readiness Index (2021) ³	ECFR European Sovereignty Index – Technology (2022) ⁴
1	Finland	Denmark ^{ESA}	Singapore ^{IA, ESA}	Finland
2	Denmark ^{ESA}	United States ^{IA, ESA}	Luxembourg	Luxembourg
3	The Netherlands	Sweden ^{IA, ESA}	Iceland	Sweden ^{IA, ESA}
4	Sweden ^{IA, ESA}	Singapore ^{IA, ESA}	United States ^{IA, ESA}	Ireland
5	Ireland	Switzerland ^{IA}	Sweden ^{IA, ESA}	The Netherlands
6	Malta	The Netherlands	Denmark ^{ESA}	Denmark ^{ESA}
7	Spain	Finland	South Korea ^{IA, ESA}	Estonia
8	Luxembourg	South Korea ^{IA, ESA}	New Zealand	Slovenia
9	Estonia	Hong Kong	Switzerland ^{IA}	Belgium ^{ESA}
10	Austria ^{IA}	Canada ^{IA, ESA}	United Kingdom ^{IA, ESA}	France ^{IA, ESA}
11	Slovenia	Taiwan ^{IA, ESA}	Estonia	Germany ^{IA, ESA}
12	France ^{IA, ESA}	Norway	The Netherlands	Cyprus
13	Germany ^{IA, ESA}	United Arab Emirates	Norway	Austria ^{IA}
14	Lithuania	Australia ^{ESA}	Ireland	Spain
15	European Union	Israel ^{IA}	Finland	Malta
• In-depth case-study countries in this report				
<p>¹ The Digital Economy and Society Index ranks EU member states based on four key dimensions: (1) Connectivity; (2) Human Capital; (3) Integration of Digital Technology; and (4) Digital Public Services. Each dimension includes a plethora of different relevant indicators. For example, the Connectivity dimension measures fixed broadband take-up, fixed broadband coverage, mobile broadband and the broadband price index.</p>				
<p>² The IMD World Digital Competitiveness Ranking ranks countries based on their performance across three key factors: (1) Knowledge; (2) Technology; and (3) Future Readiness. Each factor is divided into nine sub-factors: (1) Talent, Training and Education, Scientific Concentration; (2) Regulatory Framework, Capital, Technological Framework; and (3) Adaptive Attitudes, Business Agility, IT Integration.</p>				
<p>³ The Cisco Digital Readiness Index ranks countries based on their digital readiness, as measured by their performance across seven holistic components: (1) Basic Needs; (2) Business and Government Investment; (3) Ease of Doing Business; (4) Human Capital; (5) Start-Up Environment; (6) Technology Adoption; and (7) Technology Infrastructure. Similar to the DESI, each component ranking is determined by performance in a number of relevant indicators. For example, the Technology Adoption component includes Mobile Cellular Penetration, Internet Usage and Public Cloud Services (IT Spend Forecast).</p>				
<p>⁴ The ECFR Sovereignty Index ranks EU member states based on their contributions to European sovereignty across six 'terrains': Climate; Defence; Economy; Health; Migration; and Technology. The Technology Index defines technological sovereignty as 'the ability to shape critical technologies in accordance with the European Union's interests and values'. Technology Index scores are based on member-state contributions to critical technologies, including artificial intelligence, big data, cloud computing, semiconductors, robotics, the internet of things (IoT), high-performance computing, advanced telecommunications and cybersecurity.</p>				

Source: authors' compilation.

The results of the 2022 DESI ranking demonstrate the strength of the Nordic member states in the digital domain, with Finland, Denmark and Sweden occupying spots in the top five. Interestingly, while Finland and Denmark received comparable composite scores, each demonstrates a particular strength in a specific dimension: Finland receives a particularly strong Human Capital score, while Denmark scores highest in Connectivity. Sweden scores lower overall, with no dimension scored relatively higher than its counterparts in the top five. Meanwhile, EU political heavyweights Germany and France scored comparatively lower, although their Connectivity scores appeared comparable to the leading member states. Figure 7 displays the results of the DESI 2022 for all member states.

Figure 7 Digital Economy and Society Index (DESI), 2022
















































Source: DESI 2022, European Commission.

The IMD and Cisco rankings yield similar results, with Nordic countries again generally performing strongly in the various indicators. Interestingly, Finland ranks 15th in the Cisco Digital Readiness Index, driven largely by its poor score in the Start-Up Environment component. Unsurprisingly, the United States ranks highly in both international indices, commensurate with its GDP and large high-tech and digital sectors. Neither France nor Germany reached the top 15 of either global ranking, despite their investments in critical and emerging digital technologies. Looking beyond Europe and the US, it is striking that while several Indo-Pacific countries perform well in both digital indices, China remains absent. The use of indicators based on per capita measurements of digital skills or connectivity may fail to reflect Beijing’s strength in the digital domain, given the size of China’s population and its status as a developing country.

Indeed, China's ranks of 17 and 55, respectively, belie the strength of its booming digital enterprises and R&D environment. Similarly, India ranks 44th and 104th, respectively, despite significant investments in technology and digital projects.

Thus, while these indices provide data on a broad range of technological and digital indicators, the weight they place on individuals (for example, access to broadband and digital skills) results in rankings that do not capture the full scope of state capabilities in these domains. To address this gap, the quick scan also incorporates the Australian Strategic Policy Institute's (ASPI) Critical Technology Tracker. This tool identifies which countries lead in research on a diverse range of technological focus areas, from telecommunications to biotechnology. The ASPI bases its rankings both on the proportion of 'high-quality' research papers published and the number of high-ranking research institutions in each country. Table 3 provides a consolidated snapshot of key 'digital-enabling' technologies from the ASPI tracker. Strikingly, China dominates the field in all but one critical technology, with its research institutions generating almost one-third of all research output in each area. The previous indices do not capture this dominance, nor do they illustrate China's significant contributions to technological research and development. As noted previously, technological leadership enables digital leadership, meaning that China's research investments today will likely translate to dominance in the digital domain in the years to come. Additionally, while US research output places the United States firmly ahead of others in the Critical Technology Tracker, the United Kingdom, Germany and India consistently rank in the top five across each technology, demonstrating their consistent leadership in these areas. However, with the majority of these technologies displaying at least a medium level of Chinese monopoly risk, additional strategic investments must be made to secure Dutch (and European) DOSA.

Table 3 Key digital-enabling technologies from the ASPI Critical Technology Tracker

Technology Area	Technology	Top 5 Countries					Technology Monopoly Risk
Artificial Intelligence (AI), Computing, and Comm.	Advanced radiofrequency comm. (incl. 5G and 6G)	 29.65%	 9.50%	 5.18%	 4.89%	 4.83%	8/10 3.12 High
	Advanced optical comm.	 37.69%	 12.76%	 5.64%	 3.88%	 3.48%	8/10 2.95 Medium
	AI algorithms and hardware accelerators	 36.62%	 13.26%	 4.20%	 4.15%	 3.48%	7/10 2.76 Medium
	Distributed ledgers	 28.38%	 11.32%	 8.94%	 5.54%	 4.81%	6/10 2.51 Medium
	Advanced data analytics	 31.23%	 15.45%	 6.02%	 4.19%	 3.92%	8/10 2.02 Medium
Quantum technologies	Quantum computing	 33.90%	 15.03%	 6.11%	 5.52%	 4.13%	8/10 2.26 Medium
	Post-quantum cryptography	 30.98%	 13.30%	 6.41%	 4.73%	 3.69%	4/10 2.30 Low
	Quantum comm. (incl. quantum key distribution)	 31.47%	 16.68%	 7.58%	 6.45%	 3.81%	5/10 1.89 Low
	Quantum sensors	 23.70%	 23.27%	 7.76%	 4.29%	 4.20%	2/10 1.02 Low
<p>Technology Monopoly Risk seeks to highlight concentrations of technological expertise in a single country. It includes:</p> <ul style="list-style-type: none"> number 1 country's share of world's top 10 institutions number 1 country's lead over closest competitor (ratio of respective share of top 10% publications) a traffic-light rating: <ul style="list-style-type: none"> High = 8+/10 top institutions in no. 1 country <i>and</i> at least 3x times research lead Medium = 5+/10 top institutions in no. 1 country <i>and</i> at least 2x times research lead Low = medium criteria not met 							

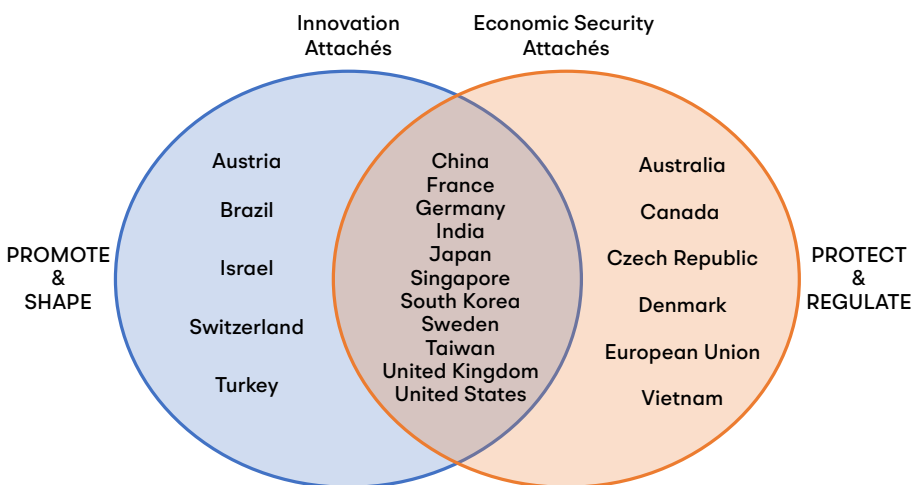
Source: authors' compilation with data from the ASPI Critical Technology Tracker.

Based on these five rankings, Finland, Sweden, Denmark, the United States, Singapore, South Korea and China stand out as digital leaders relevant to Dutch DOSA formation. Each performs well across multiple selected indices, demonstrating a broad range of digital competencies. On the other hand, Finland, Sweden, France, Germany, the United States, China, the United Kingdom and India stand out as technological leaders, as indicated by their high position in both the ECFR and ASPI rankings. Taken together, this population not only captures a broad range of digital leaders, but also the geographic technology hubs of North America, Europe and the Indo-Pacific.

3.2.2 Partners, competitors, rivals and geopolitical heavyweights

To identify relevant partner and rival countries, the postings of Dutch Innovation Attachés (IAs) and Economic Security Attachés (ESAs) yield an initial population from which to generate a sample of potential case studies. As noted in Section 2.2.1, the IA network at Dutch representations abroad seeks to connect high-technology companies, research institutions and governments with partners in in host countries. Additionally, the IA network monitors advancements in the high-technology space and provides guidance to Dutch actors attempting to enter foreign markets. These efforts correspond to the Promote line of action. Complementing these efforts are Dutch ESAs, whose Protect-oriented activities seek to monitor and address issues such as supply management and economic coercion. Figure 8 lists the countries in which the Netherlands currently posts IAs and ESAs.

Figure 8 Placement of Dutch IAs and ESAs



Source: authors' compilation.

The IA and ESA networks maintain approximately equal representation across Europe, the Americas and the Indo-Pacific, with the majority of countries falling between the partner and competitor nodes of the Partner–Rival spectrum. The only exceptions are China, Brazil and Turkey. The presence of both IAs and ESAs in China reflects its status as a geopolitical superpower, its thriving high-tech sector, growing global digital footprint and its willingness to utilise economic coercion. Turkey’s and Brazil’s inclusion in the IA network appears anomalous, as they are not technological or digital leaders in the traditional sense. However, given the size of these developing countries’ economies and their apparent willingness to engage with rivals to Europe such as China and Russia, the presence of IAs may represent an interest in building deeper partnerships to sway them away from these authoritarian allies.

Unsurprisingly, the host countries of IAs and ESAs generally perform well on the digital and technological indices discussed in section 3.2.1 above, as displayed in Table 4 below. With the exception of Brazil, India, Turkey and Vietnam, all host countries score in the top third of at least one index, although India’s strong performance in digital-enabling technologies listed in the ASPI Tracker is emblematic of its efforts to join the ranks of high-tech nations. Thus, the majority of IA and ESA countries can be considered digital and technological leaders, while these three outliers – China, Brazil and Turkey – could be considered digital and technological laggards.

Table 4 Performance of Dutch IA and ESA host countries in digital and technological indices

Country	Innovation Attaché	Economic Security Attaché	Digital indices			Technology indices	
			DESI	IMD	Cisco	ECFR	ASPI Top 5
Australia	—	✓	—	14	16	—	✓
Austria	✓	—	10	18	22	13	—
Belgium	—	✓	16	23	27	9	—
Brazil	✓	—	—	52	82	—	—
Canada	✓	✓	—	10	17	—	✓
China	✓	✓	—	17	55	—	✓
Czech Republic	—	✓	19	33	29	21	—
Denmark	—	✓	2	1	6	6	—
France	✓	✓	12	22	25	10	—
Germany	✓	✓	13	19	19	11	✓
India	✓	✓	—	44	104	—	✓
Israel	✓	—	—	15	20	—	—
Japan	✓	✓	—	29	18	—	✓
Singapore	✓	✓	—	4	1	—	—
South Korea	✓	✓	—	8	7	—	✓
Sweden	✓	✓	4	3	5	3	—
Switzerland	✓	—	—	5	9	—	—
Taiwan	✓	✓	—	11	—	—	—
Turkey	✓	—	—	54	56	—	—
United Kingdom	✓	✓	—	16	10	—	✓
United States	✓	✓	—	2	4	—	✓
Vietnam	—	✓	—	—	57	—	—
Top Third of Index		Middle Third of Index		Bottom Third of Index			

Note: See Table 2, Table 3 and Figure 7 in subsection 3.2.1 for additional information about cited indices.

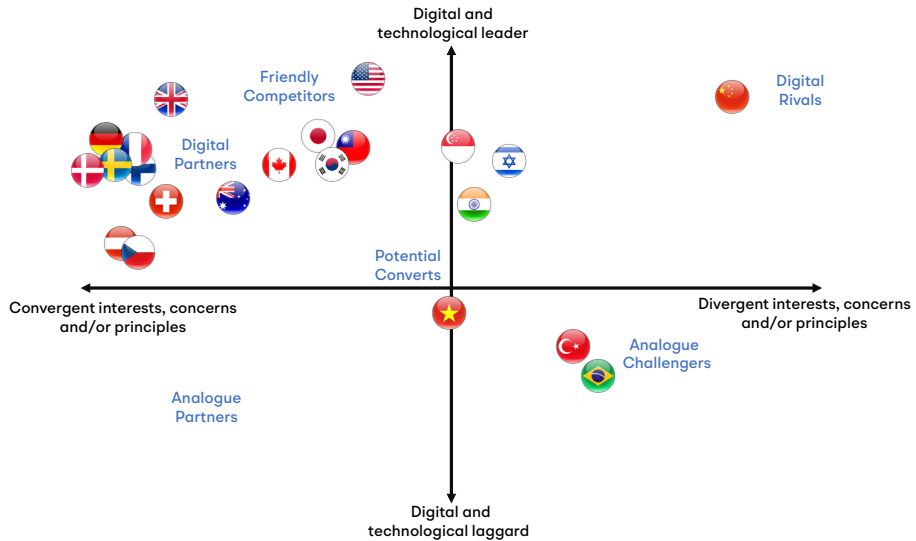
Source: authors' compilation.

Based on these placements, Germany, France, Sweden, the United States, China, Taiwan, South Korea, Japan and India stand out as significant countries for Dutch DOSA guidelines and the formulation of tangible initiatives. In addition to combining partners, competitors and rivals, this group also includes the most influential geopolitical players at the EU (Germany and France) and global (the United States and China) levels. The rapidly growing digital economies in the Indo-Pacific region, combined with the significant investments of their governments in technological innovation and development, and their important role in global digital governance and diplomacy, are further reason for the Netherlands and the EU to invest in closer ties with these countries. The presence of IAs in these countries indicates the Dutch government's interest in their technological and digital landscapes and their potential as leaders in these fields.

3.2.3 Quick scan analysis

Based on the foregoing, the quick scan yields populations of digital and technological leaders; digital and technological partners, competitors and rivals; and geopolitically significant countries. These populations – and any other countries of interest – can be further categorised based on the degree to which their interests, concerns and/or principles diverge from the Netherlands, as well as their relative strength in the digital and technological domains, as shown in Figure 9. Plotted in this manner, a number of distinct groupings emerge, each with varying degrees of relevance for formulating Dutch DOSA-related tangible initiatives. For example, the 'Digital Partners' represent the Netherlands' closest peers, both in terms of digital/technological capabilities and shared interests, while the 'Friendly Competitors' include those countries that can match the Netherlands in the digital/technological domains, but whose interests may diverge in specific areas. These countries' approaches to securing digital autonomy and sovereignty represent 'best practices' that can and should be considered. Conversely, the 'Analogue Partners' and 'Analogue Challengers' groupings are relatively less important, as they lack the digital and technological competences to inform Dutch policy effectively. Furthermore, while the placements in Figure 9 reflect digital and technological leadership as informed by the various indices cited in this report, additional indicators could be leveraged to explore these constellations of actors further.

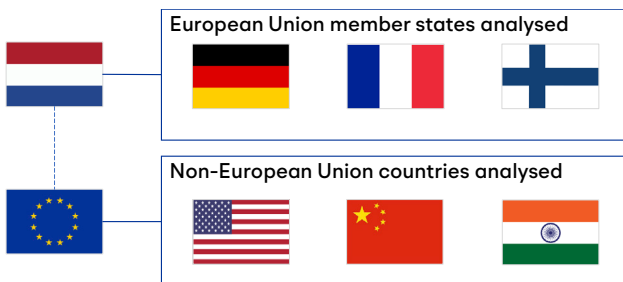
Figure 9 Quick scan of IA and ESA countries and their relationship to the Netherlands



Source: authors' compilation.

Using the quick scan exercise, this report draws its six case studies from the top half of Figure 9, as these partners, competitors and rivals capture the world's digital and technological leaders. Among the countries at the Partner end of the spectrum, Germany and France warrant additional analysis, as they represent arguably the two most influential and economically powerful EU member states. Finally, despite its relatively lower focus on cutting-edge R&D activities, Finland's strong performance in the DESI and ECFR's Sovereignty on Technology rankings, as well as its security-oriented posture (especially in light of the ongoing Russian invasion of Ukraine), ensure a unique strategic viewpoint that will inform a more comprehensive Dutch DOSA approach. Among the Netherlands' Friendly Competitors, the United States and India stand out for their geopolitical significance. The United States and, to a lesser extent, India align relatively more with the Netherlands and the EU on concerns about non-market practices and challenges to digital openness, freedom and democracy. China, as the greatest Digital Rival and a global superpower, must be carefully studied in the process of creating the Dutch DOSA approach. Figure 10 thus depicts the sample for the in-depth case study analysis, discussed in more detail in the next sections.

Figure 10 Countries included in in-depth case-study analysis



3.3 Analysis of EU member states

This section presents in-depth case studies on the EU member states that emerged from the quick scan analysis as most relevant for the purpose of informing a set of Dutch DOSA-related guidelines and tangible initiatives: Germany; France; and Finland. Each case study utilises the DTS and PS–RP frameworks introduced earlier to evaluate a selection of key policies, initiatives and strategies related to the themes of DOSA put forth by each member state. Each case study discusses the key policy initiatives of the country in question, and summarises these in a table by categorising the various items into the relevant DTS layers and PS–RP lines of action. Additionally, radar charts are used to visualise the relative significance of each member state’s investment in the five DTS layers analysed in this report. These case studies do not provide an exhaustive list of all policies and initiatives adopted at the member-state level, but rather a snapshot of items from which the Netherlands may either draw inspiration or strategise around when designing its DOSA approach.

3.3.1 Germany

As noted in the quick scan exercise in subsection 3.2.3 of this report, Germany’s influence within the EU and status as a technological leader warrant additional case-study analysis. However, Germany’s competences in advanced manufacturing and research do not compensate for its weaknesses in the digital domain. As such, Germany’s efforts to address the digital element of OSA combine Promote actions that are designed to strengthen its digital sovereignty with a strong focus on cybersecurity. Table 5 outlines a selection of key German policies and initiatives, and categorises them using the PS–RP and DTS frameworks.

Table 5 Case study of Germany: PS–RP and DTS analysis of digital and technology policies

DTS Layers	Promote and Shape (PS)	Regulate and Protect (RP)
Applications & Services	<ul style="list-style-type: none"> • European Tech Champions Initiative (National Contributor) ^{SR} • Industry 4.0 • Digital Hub Initiative • Agency for Transfer and Innovation (DATI – proposed) • Venture Tech Growth Financing Programme ^{SR} • Start-Up Strategy • Digital Strategy 2025 • AI Strategy of the Federal Government ^{SR} 	<ul style="list-style-type: none"> • Cybersecurity Strategy for Germany 2021 ^{SR} • AI Strategy of the Federal Government ^{SR}
Data	<ul style="list-style-type: none"> • Industry 4.0 • Digital Hub Initiative • Digital Strategy 2025 • Data Strategy of the Federal Government 	<ul style="list-style-type: none"> • Federal Data Protection Act (implementing GDPR) ^{SR} • Cybersecurity Strategy for Germany 2021 ^{SR} • Data Strategy of the Federal Government
Soft Infrastructure	<ul style="list-style-type: none"> • Industry 4.0 • Digital Hub Initiative • Agency for Transfer and Innovation (DATI – proposed) • Venture Tech Growth Financing Programme ^{SR} • Start-Up Strategy • Digital Strategy 2025 	<ul style="list-style-type: none"> • Cybersecurity Strategy for Germany 2021 ^{SR} • AI Strategy of the Federal Government ^{SR} • Investment screening for IT security products and technology ^{SR}
Hard Infrastructure	<ul style="list-style-type: none"> • Industry 4.0 • Digital Hub Initiative • Agency for Transfer and Innovation (DATI – Proposed) • Venture Tech Growth Financing Programme ^{SR} • Start-Up Strategy • Digital Strategy 2025 • Quantum Technology Action Concept 	<ul style="list-style-type: none"> • Cybersecurity Strategy for Germany 2021 • Prague Proposal 2019 • AI Strategy of the Federal Government ^{SR} • Investment screening for IT security products and technology ^{SR}
Raw Materials	<ul style="list-style-type: none"> • Raw Materials Strategy 2019 (further revisions forthcoming) ^{SR} • Franco-German Non-Paper on a Critical Raw Materials Act ^{SR} 	<ul style="list-style-type: none"> • Raw Materials Strategy 2019 (further revisions forthcoming) ^{SR} • Franco-German Non-Paper on a Critical Raw Materials Act ^{SR}

Source: authors' compilation.

Germany generally approaches the digital dimension of OSA through the lens of digital sovereignty, which it defines as ‘the capabilities and options of individuals and institutions to exercise their role(s) in the digital world independently, autonomously and safely’.⁸² Similar to the current Dutch focus on DOSA, this guiding principle informs many of the policies listed in Table 5 above. For example, Germany’s Cybersecurity Strategy 2021 provides key guiding principles and action areas to shape its policy in this domain through 2026, but frames them as necessary steps for achieving digital sovereignty. This document also presents cybersecurity as a joint effort by the public sector, private sector and individuals, with each group’s autonomy and the autonomy of the country given consideration. A German objective of particular interest is the creation of binding, EU-wide information and communications technology (ICT) security requirements, both to secure Europe’s critical infrastructure and to provide safety assurances to the consumer market.⁸³ Such efforts would cut across the Applications & Services, Data, Hard Infrastructure and Soft Infrastructure layers of the DTS. Improving the European cybersecurity posture would strengthen the Single Market and serve Dutch interests as well, so leveraging the Netherlands’ strength in this domain to cooperate with the Germans could contribute to DOSA. Additionally, such strategic collaboration within the EU setting could also secure German support in other policy areas of interest to the Netherlands.

German interest in digital sovereignty can also be seen in its Raw Materials Strategy, first devised in 2010.⁸⁴ While Germany possesses relatively stable and diversified supply chains for certain materials, its supply chains for critical raw materials used in many high-tech goods necessary for the green and digital transitions exhibit high degrees of supplier concentration.⁸⁵ Although the German government amended its original policy in 2019, current geopolitical trends require debate on additional changes to the strategy.⁸⁶ This evolving approach to securing its Raw Materials layer is indicative of Germany’s desire

82 German Federal Ministry of the Interior, Building and Community, [Cybersecurity Strategy for Germany 2021](#), August 2021, p. 22.

83 German Federal Ministry of the Interior, Building and Community, [Cybersecurity Strategy for Germany 2021](#), August 2021, p. 35.

84 International Energy Agency, [Raw materials strategy of the Federal Government: securing a sustainable supply of non-energy mineral raw materials for Germany](#), 31 October 2022.

85 EconPol, [How dependent is Germany on raw material imports? An analysis of inputs to produce key technologies](#), July 2022, p. 3.

86 Euractiv, [Germany to revamp raw materials strategy to tackle dependencies](#), 3 January 2023.

to enhance its digital and technological sovereignty, as access to these critical raw materials will enable further investment in advanced manufacturing and digital technologies, such as hard ICT infrastructure, green energy technologies, advanced batteries, and more.⁸⁷ Additionally, China's dominance in mining and processing critical raw materials poses a threat to German national autonomy, as it could theoretically cut off Germany's supply of these resources.

The Netherlands has an interest in the success of Berlin's measures to mitigate risk in its Raw Materials layer, as Dutch DOSA relies on access to key enabling resources. Furthermore, because of the criticality of German firms in ASML's supply chains, the Netherlands may consider collaborating with Germany to maintain consistent access to vital manufacturing inputs.

Germany's Protect actions can also be seen in its inbound investment screening regime under its Foreign Trade and Payments Act and the Foreign Trade and Payments Ordinance that was amended in May 2021. In addition to prior regulations that subjected investments in 'IT security' products to greater scrutiny,⁸⁸ the amended rules place heightened due diligence procedures on 16 activities in the high-tech sector.⁸⁹ These measures seek to protect the German Infrastructure layers of the DTS by preventing takeover of critical companies and producers by foreign firms. In a similar vein, recent rumours of potential export-control measures on chemicals used in semiconductor fabrication echo those leading up to the Netherlands' announcement in March 2023 of advanced semiconductor manufacturing equipment restrictions.⁹⁰ Germany's commitment to reducing its strategic dependencies and potentially supporting US efforts to constrain Chinese digital growth must be factored into a Dutch DOSA approach – whether in terms of policy inspiration or simply reactive positioning on these issues.

However, as evident in Table 5 above, the majority of Germany's efforts lie squarely in the Promote line of action. Over the last decade, the German government has created a plethora of strategy blueprints, initiatives and investment funds to improve its competitiveness in the technological domain

87 European Commission, [Critical raw materials for strategic technologies and sectors in the EU: a foresight study](#), 2020.

88 German Federal Ministry for Economic Affairs and Climate Action, [Investment screening](#).

89 United Nations Conference on Trade and Development – Investment Policy Hub, [Germany – FDI screening expanded over high-tech](#), 1 May 2021.

90 Reuters, [Germany plays down report on banning chip chemicals to China](#), 28 April 2023.

and to digitise its public and private sectors. Germany's Industry 4.0 strategy seeks to build upon its strong manufacturing base by implementing digital technologies such as the internet of things and AI to increase productivity and innovation.⁹¹ While some progress has been made in this arena, uptake of these solutions across the German economy remains incomplete, with the majority of medium-sized enterprises failing to implement advanced digital technologies.⁹² The Industry 4.0 strategies are complemented by the Digital Hub Initiative, which connects the business community with 12 innovation hubs around the country. These hubs each specialise in a particular digital field, including Digital Logistics, Fintech & Cybersecurity, Digital Health, Artificial Intelligence and Future Technologies.⁹³ Germany also continues to make significant investments in quantum technology, in line with its 'Quantum Technologies Action Concept'. Indeed, Germany leads EU member states in public investments in quantum computing, accounting for up to 40 per cent of expenditures.⁹⁴ Additionally, US technology firm IBM announced plans in June 2023 to build a quantum computing centre in Ehningen, the first of its kind in the EU.⁹⁵ These strategies cut across multiple layers of the DTS, representing holistic investments that seek to develop Germany into a digital leader to match its status as a frontrunner in the advanced technology domain.

Moreover, Germany has adopted a proactive industrial policy aimed at incentivising investment and start-up companies in its high-tech and digital sectors. Significantly, Germany supports the European Tech Champions Initiative ('ECTI'), which seeks to nurture the next generation of so-called unicorns⁹⁶ through investments in European venture capital firms. Administered by the European Investment Bank and building upon the work of the European Innovation Fund, the ECTI launched on 13 February 2023 with the goal of investing up to €10 billion in 'innovative companies in their growth stage'.⁹⁷

91 German Federal Ministry for Economic Affairs and Climate Action, [Industry 4.0](#).

92 German Council on Foreign Relations (DGAP), [Technology and industrial policy in an age of systemic competition](#), 9 November 2022.

93 German Federal Ministry for Economic Affairs and Climate Action, [Twelve hubs, one digital ecosystem: digital hub initiative](#).

94 McKinsey & Co., [Quantum Technology Monitor 2022](#), June 2022, p. 16.

95 Euractiv, [IBM plans first European quantum computing centre in Germany](#), 7 June 2023.

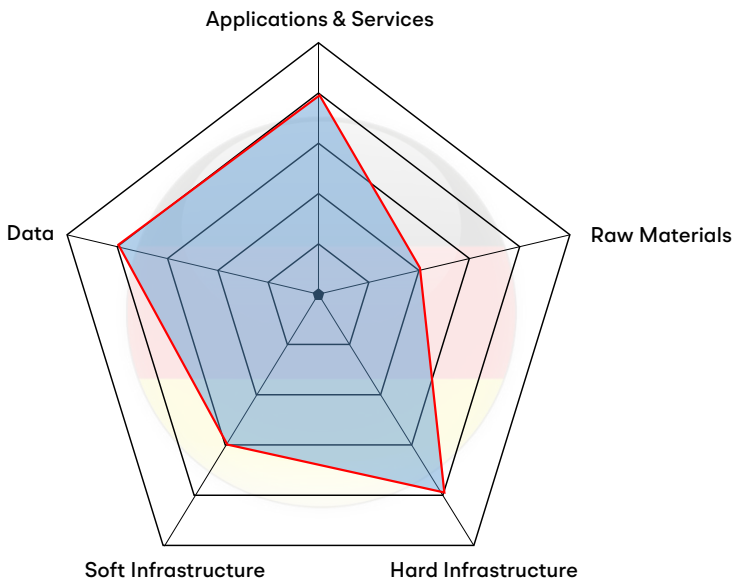
96 Generally, a company is considered a unicorn if it is valued at over US\$1 billion. This term is also heavily associated with US Silicon Valley start-up companies, many of which became investor darlings as the first 'unicorns'.

97 European Investment Fund, [ECTI: European Tech Champions Initiative](#), 13 February 2023.

Germany's direct support for this initiative demonstrates a willingness to support more actively infant companies and provide them with the funding necessary both to compete against tech giants in the US and China and to shield them from acquisition by non-European firms. This strategy runs counter to the market-oriented approach favoured by the Netherlands, which could complicate efforts to achieve a European DOSA that aligns closely with Dutch preferences. Other similar initiatives, such as the Venture Tech Growth Financing Fund and the proposed German Agency for Transfer and Innovation, are further evidence of Germany's objective of incubating high-tech companies to improve both German and European technological and digital leadership. As with its Protect actions, Germany's Promote initiatives cut across most layers of the DTS, reflecting the diverse target areas for German digital and technological development.

Figure 11 presents a radar chart to illustrate Germany's relative investment in the five DTS layers.

Figure 11 Germany's DTS profile



Source: authors' compilation.

Finally, Germany actively engages in a number of Shape activities to guide digitalisation efforts abroad. For example, the *Deutsche Gesellschaft für Internationale Zusammenarbeit* (GIZ) – the German development agency – currently engages in over 500 development projects with a digital component, each of which is designed to meet the target country’s needs.⁹⁸ Similarly, Germany is one of the most active member states in the EU’s Digital for Development (D4D) Hub initiative.⁹⁹ In addition to the value that such collaboration provides to the partner countries, Germany’s leadership in these projects allows it to build digital solutions in line with its values and vision of digitalisation. As the US–China rivalry increases the potential for two separate digital ecosystems, this development activity presents a strong alternative to Chinese digitalisation models, which increasingly forego the human-centric approach preferred by the EU. The Netherlands lags behind Germany in this arena and could improve its DOSA by expanding its development assistance to critical partner countries.

3.3.2 France

Of the EU member states in this case-study analysis, France represents the most strident voice calling for greater European strategic autonomy. Indeed, during French President Emmanuel Macron’s highly publicised state visit to Beijing in April 2023, he explicitly argued for Europe becoming an independent geopolitical actor that is beholden to neither US nor Chinese interests.¹⁰⁰ To achieve this goal in the digital domain, Macron’s France has deployed a number of policies and initiatives aimed at improving its technological and digital profile. While generally expressed at the national level, these Promote and Protect actions seek to build European strategic autonomy through strengthening France as a constituent EU member state. Furthermore, France makes liberal use of investment and incubation programmes, with an eye towards accelerating the growth of its digital and high-tech sectors. As noted in the quick scan exercise, despite its significant influence within the EU, France lags behind its peers in high-tech fields, although it is making significant investments to improve its position. Table 6 outlines a selection of key French policies and initiatives and categorises them using the PS–RP and DTS frameworks.

98 For additional information regarding the GIZ’s methodology and examples of its digital projects, see [‘Evaluation report 2022: digitalisation for development’](#).

99 Digital 4 Development Hub, [D4D in action: eight innovative projects](#).

100 Politico, [Europe must resist pressure to become ‘America’s followers’, says Macron](#), 9 April 2023.

Table 6 Case study of France: PS–RP and DTS analysis of digital and technology policies

DTS Layers	Promote and Shape (PS)	Regulate and Protect (RP)
Applications & Services	<ul style="list-style-type: none"> • International Digital Strategy ^{SR} • For a Meaningful Artificial Intelligence: Towards a French and European Strategy ^{SR} • Quantum Priority Research and Equipment Programme • New Technology Venture Accelerator • Young Entrepreneurs Initiative • French Tech ^{SR} • European Tech Champions Initiative (National Contributor) ^{SR} 	<ul style="list-style-type: none"> • National Digital Security Strategy ^{SR} • Cybersecurity Acceleration Strategy ^{SR}
Data	<ul style="list-style-type: none"> • Law of 7 October 2016 for a Digital Republic • Paris Call for Trust and Security in Cyberspace ^{SR} • International Digital Strategy • For a Meaningful Artificial Intelligence: Towards a French and European Strategy • Quantum Priority Research and Equipment Programme • New Technology Venture Accelerator • Young Entrepreneurs Initiative • French Tech ^{SR} 	<ul style="list-style-type: none"> • National Digital Security Strategy ^{SR} • Cybersecurity Acceleration Strategy ^{SR} • Data Protection Act (implementing GDPR) ^{SR}
Soft Infrastructure	<ul style="list-style-type: none"> • France Relance • National Recovery and Resilience Plan • Paris Call for Trust and Security in Cyberspace ^{SR} • International Digital Strategy • Quantum Priority Research and Equipment Programme • New Technology Venture Accelerator • Young Entrepreneurs Initiative • French Tech ^{SR} 	<ul style="list-style-type: none"> • National Digital Security Strategy ^{SR} • Cybersecurity Acceleration Strategy ^{SR}

DTS Layers	Promote and Shape (PS)	Regulate and Protect (RP)
Hard Infra-structure	<ul style="list-style-type: none"> • France Relance • National Recovery and Resilience Plan • Paris Call for Trust and Security in Cyberspace^{SR} • International Digital Strategy • Quantum Priority Research and Equipment Programme • New Technology Venture Accelerator • Young Entrepreneurs Initiative • French Tech^{SR} 	<ul style="list-style-type: none"> • National Digital Security Strategy^{SR} • Cybersecurity Acceleration Strategy^{SR}
Raw Materials	<ul style="list-style-type: none"> • Franco-German Non-Paper on a Critical Raw Materials Act^{SR} 	<ul style="list-style-type: none"> • ‘France 2030 Investment Plan’ – critical minerals investment • Franco-German Non-Paper on a Critical Raw Materials Act^{SR}

Source: authors’ compilation.

Amid the economic turmoil caused by the Covid-19 pandemic, France launched the France Relance programme. This national spending package provided funding for a number of initiatives aimed at stimulating the French economy and building its digital strengths. Key areas include ‘reshoring’ of key industries and production processes, such as electronics and industrial 5G applications, and investments in future technologies through the existing Investments for the Future programme (PIA).¹⁰¹ Created in 2010, the PIA provides capital for research and development projects using a number of different funding pools, including the National Valorisation Fund, the National Seed Fund and the French Tech Seed Fund.¹⁰² France Relance also incorporates France’s National Recovery and Resilience Plan (NRRP), which is funded via the EU’s Recovery and Resilience Facility. Of the funding provided under this programme, France devoted approximately 21 per cent to digital transition efforts, including a €1.8 billion investment in R&D for critical digital technologies, including cybersecurity, quantum computing and cloud technology.¹⁰³

101 French Ministry of Europe and Foreign Affairs, [France Relance recovery plan: building the France of 2030](#).

102 Université PSL (Paris Sciences & Lettres), [Investments for the future program](#).

103 European Commission, [France’s recovery and resilience plan](#).

In addition to these reactive efforts instigated by the Covid-19 pandemic, France pursues several other long-term strategies aimed at accelerating the development of key technologies. For example, under its Quantum Priority Research and Equipment Programme, Paris invests in ten different research projects in areas such as quantum computing, quantum algorithms, post-quantum cryptography and quantum communication. While a functioning commercial product remains elusive, this Promote action demonstrates a clear concern for the future of this critical technology. However, such engagement on future technologies also includes Regulate activities. The French AI strategy, for example, includes the goal of defining the ethical use of AI through consultation with a national advisory body and engaging in public debate.¹⁰⁴ Interestingly, this policy also specifically identifies ‘brain drain’ as a significant area of concern and seeks to build domestic networks to prevent it. These Promote efforts are further complemented by the French Tech initiative. Initially launched in 2013, this overarching programme seeks to build significantly the French start-up ecosystem, with an eye towards technology and digital companies.¹⁰⁵ In addition to financial support and incubation, French Tech includes other provisions aimed at building French digital strengths, such as an expedited visa programme for foreign start-up workers and founders.

At the European level, France has been one of the staunchest proponents of investment in European digital champions. It played a crucial role in the establishment of Gaia-X, which aims to create a federated data infrastructure based on European values. Moreover, France is one of the few EU member states that is involved in all approved Important Projects of Common European Interest (IPCEIs), including microelectronics, batteries and hydrogen.¹⁰⁶

In the Protect line of action, France’s National Digital Security Strategy stands out for its prescience regarding the current debate over the digital dimension of open strategic autonomy. Although launched in 2015, when many of the geopolitical trends discussed in this report had yet to materialise fully, this five-pronged strategy includes explicit acknowledgment of the risk of technological dependence in an increasingly digital world.¹⁰⁷ Accordingly, in

104 Digital Trade & Governance Plan, [For a meaningful artificial intelligence: towards a French and European strategy](#), 2018.

105 [La French Tech](#).

106 European Commission, [Important Projects of Common European Interest \(IPCEI\)](#).

107 French Prime Minister’s Office, [French National Digital Security Strategy](#), 2015, p. 40.

addition to objectives revolving around protection of critical infrastructure and data from threats originating in cyberspace, the French national strategy also seeks to identify a path towards European strategic autonomy. Additionally, this cybersecurity policy commits France to engaging actively in international debates on this topic and building on ‘trustworthy partnerships’.¹⁰⁸ Thus, while largely a high-level blueprint for achieving French goals in cybersecurity, France’s National Digital Security Strategy also demonstrates the country’s efforts to engage in Shape actions. These efforts have been further supplemented by the Cybersecurity Acceleration Strategy, which mobilises an additional €1 billion for a number of activities, including the development of cybersecurity solutions, improving coordination within the cybersecurity sector, and providing training in relevant skill areas for cybersecurity professionals.¹⁰⁹ Finally, France has also begun work on the Resources layer through its France 2030 Critical Minerals Investment Plan, which will mobilise €1 billion in investments towards projects that secure France’s supply of critical raw materials.¹¹⁰ Additionally, France co-published a list of policy priorities with Germany on the EU’s proposed Critical Raw Materials Act, thus demonstrating additional efforts to guide EU policy in this area.¹¹¹

This inclination can also be seen in the Paris Call for Trust and Security in Cyberspace, which consists of a series of multilateral consultations on a number of key cybersecurity issues.¹¹² By creating this forum for dialogue, France placed itself at the centre of international discussions on this key digital issue, thus providing opportunities to ‘Shape’ policy in this area. However, such efforts extend beyond the realm of cybersecurity, with French action in a number of development projects demonstrating its commitment to building partnerships that further both its national and EU-level goals. For example, France remains

108 French Prime Minister’s Office, [French National Digital Security Strategy](#), 2015, p. 40.

109 French Ministry of the Economy, Finance and Industrial and Digital Sovereignty, [Cybersecurity Acceleration Strategy](#), 3 February 2023 (in French).

110 French Ministry of the Green Transition and Cohesion and Ministry of the Energy Transition, [Investir dans la France de 2030: remise au gouvernement du rapport Varin sur la sécurisation de l’approvisionnement en matières premières minérales et ouverture d’un appel à projets dédié](#), 10 January 2022.

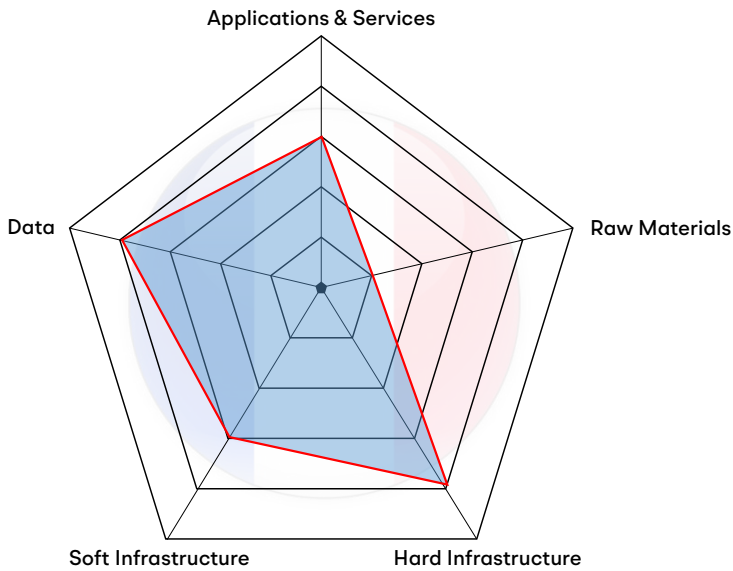
111 French Ministry of Industry and German Federal Ministry for Economic Affairs and Climate Action, [Franco-German non-paper on a Critical Raw Materials Act](#), 29 September 2022.

112 [Paris Call for Trust and Security in Cyberspace](#).

one of the most active EU member states in the D4D Hub initiative, where it serves as an initiator and/or implementor of a majority of highlighted projects.¹¹³

Figure 12 presents a radar chart to illustrate France's relative investment in the five DTS layers.

Figure 12 France's DTS profile



Source: authors' compilation.

By taking an active role in these development activities, France raises its profile as a digital leader by representing the EU abroad and builds closer ties with developing countries. In the current geopolitical climate and in the context of Macron's desire for Europe to become a third pillar of power alongside the US and China, such efforts represent crucial investments in the Shape line of action, as they increase the possibility of bringing recipient countries into the EU's vision of human-centric digitalisation. Furthermore, the French Tech initiative includes a significant international component. This initiative designates cities in third countries as 'French Tech Communities' and assists in connecting

113 Digital 4 Development Hub, [D4D in action: eight innovative projects](#).

their start-up ecosystems with those within France. For example, Nigerian city Lagos was designated a French Tech Community in January 2023, with French Minister of State for Development, Francophonie and International Partnerships Chrysoula Zacharopoulou characterising the city as the heart of African innovation.¹¹⁴ This networking improves market access for companies situated in the French Tech Communities and further ‘Promotes’ France as a location for high-tech investments.¹¹⁵ Furthermore, the focus of these initiatives and many D4D projects represents a strategic effort to improve French and European ties with Africa. The continent is increasingly becoming a new front in the US–China rivalry, thus necessitating a commensurate increase in productive engagement.

3.3.3 Finland

The Finnish approach to the digital dimension of OSA reflects a strong orientation towards the Promote line of action across all layers of the DTS, while simultaneously drawing on Finland’s long-standing ‘security of supply’ tradition to inform its Protect actions. Notably, these policy preferences generally do not supersede Helsinki’s open-market orientation. As a result, Finland remains aligned with the Netherlands and other like-minded countries on the ‘open’ element of OSA.¹¹⁶ Finland also adheres to the EU vision of human-centred digitalisation, resulting in a particular focus on the Data layer that emphasises improving data usage, sharing and protection. Table 7 outlines a collection of significant Finnish policy documents that are relevant for understanding Finland’s approach to the digital dimension of OSA.

114 *Business Day*, [French tech community launched in Lagos](#), 5 June 2023.

115 French Ministry of Europe and Foreign Affairs, [Promoting and supporting French innovation](#), July 2021.

116 Swedish Institute of International Affairs, [Controlling critical technology in an age of geo-economics: actors, tools and scenarios](#), 2023, p. 35.

Table 7 Case study of Finland: PS–RP and DTS analysis of digital and technology policies

DTS Layers	Promote and Shape (PS)	Regulate and Protect (RP)
Applications & Services	<ul style="list-style-type: none"> • Artificial Intelligence Programme ^{SR} 	<ul style="list-style-type: none"> • Finland’s Cybersecurity Strategy 2019
Data	<ul style="list-style-type: none"> • Artificial Intelligence Programme ^{SR} • Act on the Secondary Use of Health and Social Data ^{SR} • Government Resolution on Technology Policy ^{SR} 	<ul style="list-style-type: none"> • Government Decision on the Objectives of Security of Supply • Finland’s Cybersecurity Strategy 2019 • General Data Protection Regulation ^{SR} • Data Protection Act ^{SR}
Soft Infrastructure	<ul style="list-style-type: none"> • Artificial Intelligence Programme ^{SR} • Government Resolution on Technology Policy ^{SR} 	<ul style="list-style-type: none"> • Government Decision on the Objectives of Security of Supply • Finland’s Cybersecurity Strategy 2019
Hard Infrastructure	<ul style="list-style-type: none"> • Turning Finland into the world leader in communications networks – Digital Infrastructure Strategy 2025 • Government Resolution on Technology Policy ^{SR} • National Battery Strategy 2025 ^{SR} 	<ul style="list-style-type: none"> • Government Decision on the Objectives of Security of Supply • Finland’s Cybersecurity Strategy 2019 • Turning Finland into the world leader in communications networks – Digital Infrastructure Strategy 2025
Raw Materials	<ul style="list-style-type: none"> • Report of Investigation 219: Discovery potential of high-tech metals and critical minerals in Finland 	<ul style="list-style-type: none"> • Government Decision on the Objectives of Security of Supply • EU policy and strategy for raw materials • Critical metals and minerals in Fennoscandia • Report of Investigation 219: Discovery potential of high-tech metals and critical minerals in Finland

Note: SR refers to Shape and Regulate initiatives.

Source: authors’ compilation.

A key document guiding Finland’s approach to the digital dimension of OSA is the 2018 Government Decision on the Objectives of Security of Supply, which represents a holistic Protect action encompassing multiple layers of the DTS. This policy document defines security of supply as ‘the safeguarding of the critical production, services and infrastructure necessary for the livelihood of the

population, the national economy and the national defence in cases of serious incidents and emergencies'.¹¹⁷ While originating from Cold War-era efforts to ensure Finnish physical security and resilience,¹¹⁸ the Government Decision now explicitly highlights Finland's 'digital society'. It expands the scope of the security-of-supply concept to include critical infrastructure (including hard and soft digital infrastructure), digital financial services, logistics networks, mass media and the various supply chains that implicate these areas.¹¹⁹ Consequently, this strategy document directs the Finnish government to 'Protect' various areas that correspond to elements of the Data, Soft Infrastructure, Hard Infrastructure and Resource layers of the DTS. Critically, Finland achieves its security of supply through voluntary public-private cooperation. While some companies do face certain mandated emergency stock requirements, the Finnish government's efforts to educate companies on their role in this policy and to provide horizontal and vertical networking opportunities represent a novel approach not seen in the Netherlands. Expanding the scope of public-private partnerships to achieve DOSA could greatly improve the Netherlands' strategic position in the long term.

Complementing this policy, the Cybersecurity Strategy 2019 and the Finnish government's Resolution on the Cybersecurity Development Programme commit significant resources towards securing the digital landscape, both to protect Finnish interests and to create a more hospitable environment for R&D and business in the digital and technology domains. The Cybersecurity Strategy also highlights Finnish engagement at both the EU and international levels on this topic. Through these forums, Finland seeks to shape European cybersecurity standards and coordinate with third-country partners to address various digital threats. Taken together, these policies reflect investments in the Applications & Services, Data, Soft Infrastructure and Hard Infrastructure DTS layers. Given the Netherlands' strength and activity in this domain, a Dutch DOSA approach could benefit significantly from deeper coordination and partnership with Finland on Protect actions in the cybersecurity realm.

117 Finish Government, [Government Decision on the Objectives of Security of Supply \(1048/2018\)](#), 5 December 2018, p. 1.

118 Finnish Institute of International Affairs, [The EU and Finland's security of supply: a 'turn' in EU thinking provides new opportunities, but significant differences remain](#), January 2022, p. 3.

119 Finish Government, [Government Decision on the Objectives of Security of Supply \(1048/2018\)](#), 5 December 2018, pp. 5-6.

While these broad-based initiatives simultaneously address multiple DTS layers, Finland also employs several Protect measures that are targeted to individual layers. Beyond cybersecurity, the Data Protection Act, which implements the General Data Protection Regulation, ensures the protection of the Finnish Data layer at the end-user level. Furthermore, the Finnish Innovation Fund SITRA engages in ongoing research regarding the proliferation and use of individual data, including a 2022 study on how the personal data of key Finnish policymakers could be leveraged to gain influence and shape public debates.¹²⁰ In terms of Hard Infrastructure, Finland's Digital Infrastructure Strategy 2025 not only highlights the need to 'Promote' the expansion of Finnish connectivity and investments in emerging technologies, but also emphasises that all new digital infrastructure projects must incorporate a strong security component.¹²¹ Finally, in an effort to protect the Finnish and European Raw Materials layer, Finland continues to assess its extensive deposits of critical raw materials and expand its domestic mining operations.¹²² However, these efforts may have stagnated, as Finland still relies upon imports for the majority of its resource needs relevant to digital technologies. In other words, Finland appears willing to accept the risks associated with importing the majority of its critical raw materials.

Finland's Promote actions reflect a relatively less holistic approach compared to its Protect initiatives, but do implicate every layer of the DTS to varying degrees. The Artificial Intelligence Programme represents the most cross-cutting Promote policy, as it implicates the Applications & Services, Data and Soft Infrastructure layers. Across the Artificial Intelligence Programme's eleven focus areas, the Finnish government seeks to spur investment in and adoption of AI technologies by creating favourable regulatory and market conditions, especially for small and medium-sized enterprises.¹²³ Finland also seeks to 'Promote' its Data layer by reforming data-sharing guidelines, thus allowing research institutions and the government to collate and utilise individual-level data.¹²⁴ Furthermore, these efforts designate Findata as Finland's information permit authority, providing

120 SITRA, [Digipower investigation](#).

121 Finnish Ministry of Transport and Communications, [Turning Finland into the world leader in communications networks – Digital Infrastructure Strategy 2025](#), 2019.

122 Geological Survey of Finland, [Report of Investigation 219: discovery potential of hi-tech metals and critical minerals in Finland](#), 2015.

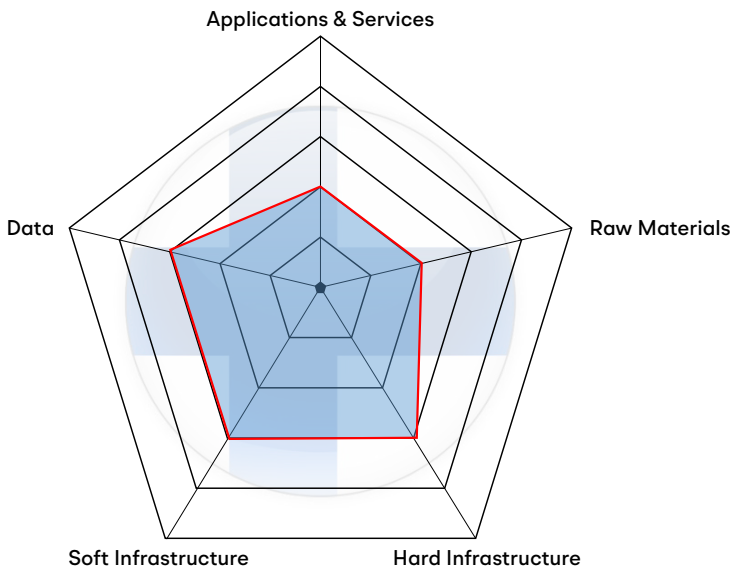
123 Finnish Ministry of Economic Affairs and Employment, [Leading the way into the age of artificial intelligence: final report of Finland's Artificial Intelligence Programme 2019](#), 2019.

124 University of Eastern Finland, [Act on the Secondary Use of Health and Social Data](#), 2019.

an institutional framework for giving qualified parties access to these valuable data streams. Finland also makes investments in Promote activities in the Hard Infrastructure layer, such as the National Battery Strategy 2025.¹²⁵ This policy seeks to utilise Finland’s abundant lithium resources to expand its research, development and manufacturing capacity for advanced battery technologies. Additionally, the state-owned and controlled Technical Research Centre of Finland (VTT) pursues emerging technologies and provides infrastructure for the academic and private sectors to conduct research. For example, the VTT’s quantum infrastructure programme seeks to provide enabling technologies to various companies and institutions engaged in this critical research area.¹²⁶ This focus on developing industries that supply digital-enabling infrastructure and technologies may complement Dutch DOSA implementation, with the Netherlands seeking to lead innovation in these emerging technologies.

Figure 13 presents a radar chart to illustrate Finland’s relative investment in the five DTS layers.

Figure 13 Finland’s DTS profile



Source: authors' compilation.

125 Finnish Ministry of Economic Affairs and Employment, [National Battery Strategy 2025](#), 2021.

126 VTT Technical Research Centre of Finland, [Quantum technology infrastructure](#).

Notably, Finland opposes significant Promote or Protect measures that interfere with open markets, such as new export controls or more rigorous inbound and outbound investment screening processes. While the Netherlands generally shares this orientation towards open markets, the announcement of Dutch export controls on semiconductor manufacturing equipment in early 2023 demonstrates some degree of difference in national approaches – likely resulting from differences in industrial strengths. Improving Dutch understanding of Finnish practices, such as security of supply and Finland’s approach to public–private sector cooperation, could ensure that these divergences in policy preferences do not limit the scope of cooperation on issues relevant to DOSA.

3.4 Analysis of non-EU countries

This section presents in-depth case studies on the non-EU countries that are most relevant to consider when designing a Dutch DOSA implementation plan: the United States; China; and India. Similarly to the analysis of EU member states made in section 3.3, this section uses the DTS and PS–RP frameworks, and presents a simplified assessment per country using summary tables and radar charts.

3.4.1 The United States of America

The United States continues to make deep investments in a variety of digital areas, commensurate with both its role as a military and economic superpower, and its intensifying rivalry with China. The US approach to the issue of digital autonomy can be characterised by intense efforts to promote investment in critical emerging technologies, while simultaneously securing its supply chains of both critical materials and intermediate inputs, such as semiconductors. Furthermore, US has not shied away from deploying Protect measures such as export controls against China to dampen its ability to compete. Given the significance of the United States to both the Netherlands and the EU, the Dutch should not only monitor the US approach, but should ensure that any escalation of Washington’s Shape and Protect lines of action directed towards Beijing do not constrain Dutch and European autonomy.

While Washington does not have a consolidated strategy or policy for digital sovereignty, a range of policies and strategies on various sub-sets constitute a concerted effort to maintain US leadership by securing access to critical technologies, fortifying US supply chains of critical raw materials and inputs,

fostering innovation and strategic partnerships, and strengthening the US’s cybersecurity footing. Additionally, the US strategy incorporates Protect measures in the form of export controls that are designed to curtail Beijing’s access to semiconductors and prevent the further development of domestic Chinese chip development. By restricting its primary rival’s access to these critical components, the United States hopes to slow, or halt, China’s research and development efforts in a variety of digital technologies. Significant examples of such measures are summarised in Table 8 using the PS–RP framework.

Table 8 Case study of the United States: PS–RP and DTS analysis of digital and technology policies

DTS Layers	Promote and Shape (PS)	Regulate and Protect (RP)
Applications & Services	<ul style="list-style-type: none"> National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems United States Government National Standards Strategy for Critical and Emerging Technologies ^{SR} 	<ul style="list-style-type: none"> National Cybersecurity Strategy ^{SR} M-22-09: Moving the US Government Toward Zero Trust Cybersecurity Principles ^{SR} M-22-18: Memorandum for the Heads of Executive Departments and Agencies ^{SR}
Data	<ul style="list-style-type: none"> United States Government National Standards Strategy for Critical and Emerging Technologies ^{SR} 	<ul style="list-style-type: none"> National Cybersecurity Strategy ^{SR} National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems M-22-09: Moving the US Government Toward Zero Trust Cybersecurity Principles ^{SR} Foreign Investment Risk Review Modernization Act ^{SR}
Soft Infra-structure	<ul style="list-style-type: none"> National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems United States Government National Standards Strategy for Critical and Emerging Technologies ^{SR} 	<ul style="list-style-type: none"> National Cybersecurity Strategy ^{SR} M-22-09: Moving the US Government Toward Zero Trust Cybersecurity Principles ^{SR}

DTS Layers	Promote and Shape (PS)	Regulate and Protect (RP)
Hard Infra-structure	<ul style="list-style-type: none"> • Creating Helpful Incentives to Produce Semiconductors and Science Act of 2022 ('CHIPS Act') • Bipartisan Infrastructure Law • Defense Production Act Title III: Presidential Determination for Printed Circuit Boards and Advanced Packaging Production Capability • National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems • US–EU Trade and Technology Council (TTC) • US–India initiative on Critical and Emerging Technology (iCET) • United States Government National Standards Strategy for Critical and Emerging Technologies ^{SR} 	<ul style="list-style-type: none"> • National Cybersecurity Strategy ^{SR} • Chip 4 (United States, Japan, South Korea, Taiwan) • Bureau of Industry and Security (BIS) Export Administration Regulations (i.e. export controls) ^{SR} • BIS Entity List
Raw Materials	<ul style="list-style-type: none"> • US Strategy Toward Sub-Saharan Africa ^{SR} • USAID Digital Strategy 2020–2024 ^{SR} 	<ul style="list-style-type: none"> • Executive Order on America's Supply Chains • FACT SHEET: Securing a 'Made in America' Supply Chain for Critical Minerals

Source: authors' compilation.

Note: SR refers to Shape and Regulate initiatives.

The National Cybersecurity Strategy, published in March 2023, represents the most significant contribution to what could be called a US approach to open strategic autonomy in the digital domain, and strengthens the Data, Hard Infrastructure and Raw Materials layers of the DTS.¹²⁷ Building upon a number of prior cybersecurity measures under the Trump and Biden administrations, this Protect strategy combines efforts to secure American infrastructure and data from cyber-attacks, with measures to incentivise research and development and investment in cutting-edge digital technologies. Additionally, the document emphasises the need to leverage and expand trusted

127 The White House, [National Cybersecurity Strategy](#), 1 March 2023.

international partnerships to secure digital environments and supply chains providing the Raw Materials and Hard Infrastructure to facilitate these digital initiatives. This multi-pronged approach illustrates Washington's ambitions in the digital domain, its commitment to maintaining technological and digital supremacy and its capacity to pursue numerous objectives to secure digital autonomy simultaneously.

In terms of Soft Infrastructure and Applications & Services, all US federal agencies are required to adhere to the National Institute of Standards and Technology (NIST) guidance on the Secure Software Development Framework (SSDF).¹²⁸ In practice, this requires agencies to obtain attestations from any third-party developers that they meet the standards laid out in the NIST SSDF, which covers several areas of software development, deployment and maintenance. The goal of the SSDF and the guidance are to guard against potential digital vulnerabilities in the United States and to secure software supply chains to ensure that US federal agencies are using only trusted products from trusted vendors.¹²⁹

Complementing this evolving national strategy, the Creating Helpful Incentives to Produce Semiconductors and Science Act of 2022 (known as the 'CHIPS Act') and the Bipartisan Infrastructure Law comprise key elements of the United States' Promote line of action in the Hard Infrastructure layer. Broadly, the CHIPS Act seeks to increase investments in the US's domestic semiconductor manufacturing sector, facilitate R&D and the commercialisation of 'leading-edge' technologies – including quantum, AI, clean energy and nanotechnology – and increase the size and inclusivity of the United States' STEM labour force.¹³⁰ The bill devotes US\$280 billion to these efforts, with US\$200 billion directed towards R&D and workforce efforts. Additionally, US\$4 billion of the semiconductor funding allocated by the CHIPS Act is earmarked for the

128 US Department of Commerce, [M-22-18: Memorandum for Heads of Executive Departments and Agencies: enhancing the security of the software supply chain through secure software development practices](#), 14 September 2022.

129 A potential factor in the development of the SSDF could be the SolarWinds hack experienced by the United States in 2020. This incident stemmed from hostile cyber actors inserting malicious code into a routine software update published by SolarWinds, one of the US government's software vendors. For additional information, see: NPR, [A 'worst nightmare' cyberattack: the untold story of the SolarWinds hack](#), 16 April 2021.

130 US Congress, [H.R. 4346 – Chips and Science Act](#), 8 September 2022.

US military and the State Department, with an eye towards national security applications in the semiconductor and telecommunications sectors.¹³¹ Similarly, the Bipartisan Infrastructure Law allocates US\$65 billion of the nearly US\$1.2 trillion infrastructure fund to improving US broadband coverage. Taken together, these pieces of legislation represent massive investments in US Hard Infrastructure, which will speed US digitalisation and create an environment that is friendly to digital innovation. Furthermore, these measures represent key enablers for the Biden administration's Inflation Reduction Act (IRA). This spending bill not only seeks to accelerate the United States' green transition, but also deploys a number of incentives to facilitate the reshoring of manufacturing. While the IRA does not directly fund digital projects, it represents a broader effort by the United States to secure its strategic autonomy, thus making investments under the CHIPS Act and Bipartisan Infrastructure Law key components of the broader US strategy.

The United States also continues to invest heavily in the Raw Materials layer of the DTS through a number of Protect measures. For example, the Executive Order on America's Supply Chains (of 24 February 2021) compels US federal department heads to conduct a 100-day review of critical supply chains within their jurisdictions, including a Commerce Department report on semiconductor manufacturing and advanced packaging and a Defense Department report on critical minerals and other strategic minerals (for example, rare-earth elements).¹³² Additionally, the Executive Order requires each federal department to submit their findings with additional policy recommendations for improving the resilience of these supply chains. Following the implementation of these Protect measures, Washington announced a number of new funded projects to increase the resilience of the United States' critical mineral supply chains, including funding for a project to separate and process heavy rare-earth elements to establish a full end-to-end domestic permanent-magnet supply chain, the development of sustainable domestic lithium extraction, expanding refining facilities for battery inputs, updates to the federal list of critical minerals, building national stockpiles of critical minerals and expanding the processing capacity of domestic light rare-earth elements.¹³³

131 McKinsey & Co., [The CHIPS and Science Act: here's what's in it](#), 4 October 2022.

132 The White House, [Executive Order on America's Supply Chains](#), 24 February 2021.

133 The White House, [Fact sheet: securing a Made in America supply chain for critical minerals](#), 22 February 2022; and US Department of Defense, [DOD announces rare earth element award to strengthen domestic industrial base](#), 1 February 2021.

Additionally, the United States leverages its strategic partnerships to secure various DTS layers, such as in the US Strategy Toward Sub-Saharan Africa, which was introduced in August 2022.¹³⁴ This strategy document outlines the Biden administration's diplomatic and economic approach to the region, as well as its plans to engage in a number of projects and investment opportunities to assist its African partners' development. While the document primarily focuses on development assistance activities, it mentions in several sections 'critical minerals' and the need to secure supply chains, highlighting that Washington not only approaches this element of DOSA through domestic capacity-building, but also through strategic competition in other regions to secure access to critical inputs. This new Africa strategy and a series of accompanying diplomatic efforts (such as the US–Africa Leaders Summit,¹³⁵ US Vice-President Kamala Harris's multi-country tour in April 2023,¹³⁶ and the US State Department's participation in the Africa Fintech Conference¹³⁷) appear designed to secure US interests on the African continent and to facilitate deeper integration of African partners into new US value chains.

Separately, in the Indo-Pacific region, US talks in February 2023 between the so-called 'Chip 4' partners (US, Japan, South Korea and Taiwan) concerned a proposed 'early-warning system' that the countries would deploy to alert one another of any disruptions to the semiconductor supply chain. Under this scheme, Taiwan and South Korea would focus their monitoring efforts on manufacturing, Japan on materials, and the United States on market trends.¹³⁸ Similarly, as noted previously, the United States coordinated efforts with the Netherlands and Japan on the imposition of export controls against China. Taken together, these examples represent efforts by the United States to *regulate* further the digital landscape abroad by using its diplomatic and economic influence to secure strategic partnerships and to constrain its rival's access to digital-enabling technologies.

However, while engaged in numerous Shape activities, the United States' Regulate profile lags behind other actors. While the executive branch can impose rules and standards on its departments and agencies through the use of

134 The White House, [US Strategy toward Sub-Saharan Africa](#), August 2022.

135 US Department of State, [US–Africa Leaders Summit Overview](#), 2022.

136 Associated Press, [Vice President Harris' trip aims to deepen US ties in Africa](#), 1 April 2023.

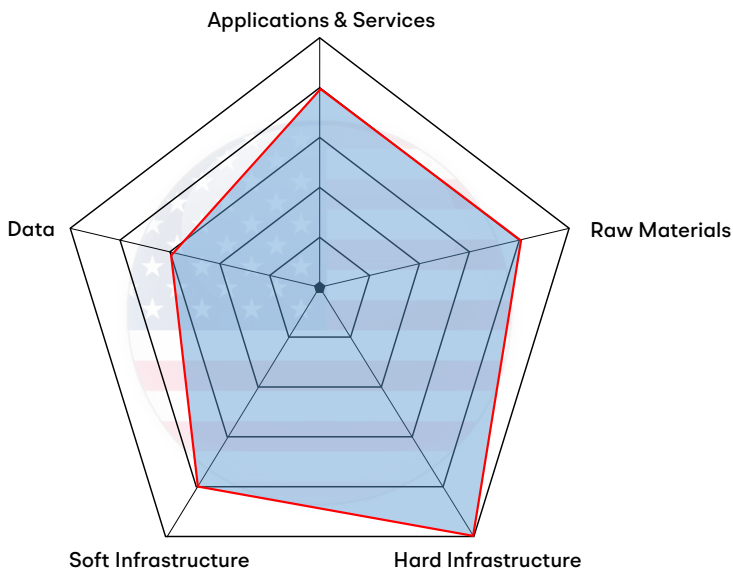
137 US Department of State, [State Department partners with Africa Fintech Summit](#), 10 April 2023.

138 Bloomberg, [US, Asian Partners discussed supply chains in 'Chip 4' talks](#), 26 February 2023.

executive orders, legislative action at the US federal level remains elusive. The House of Representatives introduced the American Data Privacy and Protection Act in June 2022, which would provide GDPR-style protections, but the bill has not yet been passed. From a data-protection and privacy perspective, the most significant *regulatory* efforts are actually occurring at the US state level. The 2018 California Consumer Privacy Act and its 2020 amendments create a strong data-protection regime for individuals, including the right to opt out of data sale-and-sharing models.¹³⁹ Eight other US states have adopted similar measures, but the lack of federal action creates significant disparities from jurisdiction to jurisdiction.¹⁴⁰

Figure 14 presents a radar chart to illustrate the United States' relative investment in the five DTS layers.

Figure 14 United States of America's DTS profile



Source: authors' compilation.

139 State of California Department of Justice, [California Consumer Privacy Act \(CCPA\)](#), 10 May 2023.

140 International Association of Privacy Professionals, [US State Privacy Legislation Tracker](#), 19 June 2023.

Thus, the United States' approach to digital autonomy relies equally upon the Promote and Protect lines of action, while making strong attempts to *shape* elements of the digital domain directly on an international scale. However, these efforts are not matched by significant domestic *regulatory* efforts outside of cybersecurity matters, perhaps because of a combination of political gridlock and lobbying efforts by companies that rely on easy access to US consumer data. Significantly, the lack of a coherent *regulatory* regime for data privacy and protection leaves a gap in the United States' capacity to engage in *Shape* actions in this area. This inactivity makes EU efforts to *shape* global standards and principles related to the Data layer all the more important. At the same time, the EU would be wise to invest in greater engagement with the growing group of actors in the United States that is now willing to act on *regulation*. In other areas of the Stack, the Netherlands and Europe more broadly should actively engage with the United States, not only because of its significance as an economic and security partner with many shared values, but also because of the sheer size of its digital landscape. Any success in *shaping* US policy in line with European values could drastically increase the scope of Europe's geopolitical influence and positively impact its efforts in other critical regions, such as the Indo-Pacific.

3.4.2 China

As the second great player in the current geopolitical realignment, China's policies in the digital and technological domains require careful consideration at both the Dutch and European levels. The size of China's economy, its significance as an export market for European goods,¹⁴¹ and its dominance in the rare-earth metals market,¹⁴² among other factors, mean that any shifts in Chinese policy will have significant downstream impacts on Dutch DOSA. This is particularly important, as China and Europe have different interpretations of government intervention in the economy, as well as of digital rights and principles, and they increasingly oppose each other on broader political issues – from the war in Ukraine to the international position of Taiwan. Similar to the United States, Beijing's current policies and initiatives relevant to DOSA combine a number of measures in both the Promote and Protect lines of action, with a heavy emphasis on building China's capacity in a number of emerging technologies. Table 9 below outlines a selection of key Chinese policies and initiatives and categorises them using the PS–RP and DTS frameworks.

141 German Council on Foreign Relations (DGAP), [Managing risks in the EU–China economic relationship](#), November 2022, p. 3.

142 Foreign Policy Research Institute, [China's rare earth metals consolidation and market power](#), 2 March 2022.

Table 9 Case study of China: PS–RP and DTS analysis of digital and technology policies

DTS Layers	Promote and Shape (PS)	Regulate and Protect (RP)
Applications & Services	<ul style="list-style-type: none"> • 14th Five-Year Plan for National Informatisation • New Generation AI Development Plan • China Standards 2035 ^{SR} • National Standardisation Development Action Plan • Plan for the Overall Layout of Building a Digital China ^{SR} • New Generation Artificial Intelligence Development Plan 2017 	<ul style="list-style-type: none"> • Measures for the Management of Generative Artificial Intelligence Services ^{SR}
Data	<ul style="list-style-type: none"> • 14th Five-Year Plan for National Informatisation • Plan for the Overall Layout of Building a Digital China ^{SR} • New Generation Artificial Intelligence Development Plan 2017 • Global Data Security Initiative ^{SR} 	<ul style="list-style-type: none"> • Personal Information Protection Law ^{SR} • Data Security Law ^{SR} • Cybersecurity Law ^{SR} • Plan for the Overall Layout of Building a Digital China • Measures for the Management of Generative Artificial Intelligence Services ^{SR}
Soft Infrastructure	<ul style="list-style-type: none"> • 14th Five-Year Plan for National Informatisation • New Generation AI Development Plan • Digital Silk Road ^{SR} • China Standards 2035 ^{SR} • National Standardisation Development Action Plan • Plan for the Overall Layout of Building a Digital China ^{SR} • National Science and Technology Innovation 2030 – Major programme of ‘New Generation of Artificial Intelligence’ 2022 • Public funding programmes and instruments for semiconductor industry • New Generation Artificial Intelligence Development Plan 2017 • Public funding programmes and instruments for quantum industry 	<ul style="list-style-type: none"> • Cybersecurity Law ^{SR} • Plan for the Overall Layout of Building a Digital China

DTS Layers	Promote and Shape (PS)	Regulate and Protect (RP)
Hard Infra-structure	<ul style="list-style-type: none"> • 14th Five-Year Plan for National Informatisation • Made in China 2025 • New Generation AI Development Plan • Digital Silk Road ^{SR} • China Standards 2035 ^{SR} • National Standardisation Development Action Plan • Plan for the Overall Layout of Building a Digital China • National Science and Technology Innovation 2030 – Major program of ‘New Generation of Artificial Intelligence’ 2022 • Public funding programmes and instruments for semiconductor industry • New Generation Artificial Intelligence Development Plan 2017 • Public funding programmes and instruments for quantum industry 	<ul style="list-style-type: none"> • Cybersecurity Law ^{SR} • 35 Key ‘Stranglehold’ Technologies
Raw Materials		<ul style="list-style-type: none"> • Critical raw material extraction and processing quotas

Note: SR refers to Shape and Regulate initiatives.

Source: authors’ compilation.

On 28 December 2021, the Chinese government published the 14th Five-Year Plan for National Informatisation. This policy document serves as a roadmap, outlining ten areas for digital development, key performance indicators (KPIs) and 2025 targets, and the actionable steps necessary to achieve the desired outcomes. These development areas target all but the Raw Materials layer of the DTS and emphasise the expansion of both Hard and Soft Infrastructure, improving the availability and use of Data, and expanding the use of digital Applications & Services across the public and private sectors. Additionally, they stress increasing innovation in the digital and technological domains, and implementing both Belt and Road and Digital Silk Road projects to improve

digital infrastructure and interoperability abroad.¹⁴³ In line with this blueprint, the Chinese government in February 2023 released its Plan for the Overall Layout of Building a Digital China, which outlines progress made towards the 2025 targets and provides additional steps to achieve them. Furthermore, this 14th Five-Year Plan also includes a significant component related to the Digital China strategy's international component, which emphasises China's willingness and intent to participate in international forums related to digital matters and to increase its cooperation with other countries in this domain.¹⁴⁴ This external-facing dimension could be significant for Dutch DOSA, as it may represent the opening salvo in Beijing's attempts to export its vision of digital development and governance. Chinese success in this area could result in global norms that fail to reflect the EU's vision of human-centric digitalisation.

To operationalise these high-level strategies, the Chinese government is pursuing its digital goals through a number of Promote actions. Of particular note are its efforts in three key technologies, each of which heavily implicate digital autonomy: semiconductors; artificial intelligence; and quantum technologies, such as quantum computing, quantum communications and post-quantum cryptography. Support for China's domestic semiconductor industry can be traced back to the 'Made in China' initiative launched in 2015. This broad industrial policy seeks to reduce China's dependence on foreign imports across a variety of industries and particularly in high-tech sectors dealing in digital-enabling technologies.¹⁴⁵ 'Made in China' supports the semiconductor industry through a number of national and state-level investment funds that contributed over US\$100 billion from 2014 to 2020.¹⁴⁶ Additionally, China has provided a number of private-sector incentives such as tax breaks, favourable interest rates and new financial instruments to spur additional investment in foundries and chip designers. These represent significant investments in the Hard and Soft Infrastructure layers. Although China still lags behind seasoned manufacturers and faces fresh challenges from US-led import controls, the growth of its domestic manufacturing capacity for these critical components remains strong.

143 DigiChina (Stanford Cyber Policy Center), [Translation: 14th Five-Year Plan for National Informatisation](#), December 2021.

144 DigiChina (Stanford Cyber Policy Center), [Translation: 'Plan for the overall layout of building a digital China'](#), 3 March 2023.

145 Institute for Security and Development Policy, [Made in China 2025: background](#), June 2018.

146 Bruegel, [Lessons for Europe from China's quest for semiconductor self-reliance](#), 18 November 2022.

Similar Promote actions in the AI and quantum fields also contribute to Beijing's technological leadership through investments in the Hard and Soft Infrastructure layers. Under the guiding principles of the New Generation Artificial Intelligence Development Plan 2017, which is a blueprint for the development of the Chinese AI sector through 2017, the Ministry of Science and Technology launched the National Science and Technology Innovation 2030 – major programme of 'New Generation of Artificial Intelligence' 2022. This provides up to US\$2.8 million of public funding for AI projects in any of 16 research areas.¹⁴⁷ China's quantum sector also receives support from the government, with China's 14th Five-Year Plan allocating up to US\$15 billion to quantum technology research and development, thus exceeding EU investments by a factor of two and US investments by a factor of eight.¹⁴⁸ In line with the novelty of quantum technology, the Chinese government has also invested in human capital by creating new higher-education degree programmes for quantum-related disciplines.

China complements these Promote actions with a variety of Protect actions, exemplified most famously in its controversial Data Security and Cybersecurity Laws. China's Data Security Law, passed on 10 June 2021, creates 'core national' and 'important' data classifications, each of which carries specific handling requirements.¹⁴⁹ Critically, these classifications are vaguely defined, allowing the Chinese government to apply them at its discretion.¹⁵⁰ The 'mishandling' of such data carries heavy financial penalties and risks criminal charges, further tightening China's control of its national data through this strict *regulatory* regime. The Cybersecurity Law was passed in 2017 and includes similarly strict requirements for handling data and securing networks and digital infrastructure. This scope differs somewhat from the Data Security Law, as it places greater emphasis on the requirements for network operators. However, some of its provisions represent equally strong Protect measures, utilising ambiguity to a similar effect. Specifically, Articles 28 and 58 compel network operators to

147 Chinese University of Hong Kong, [Notification of application for National Science and Technology Innovation 2030 – major programme of 'New Generation of Artificial Intelligence' 2022](#), 18 August 2022.

148 McKinsey & Co., [Quantum Technology Monitor 2022](#), June 2022, pp. 17–18.

149 DigiChina (Stanford Cyber Policy Center), [Translation: Data Security Law of the People's Republic of China \(effective 1 Sept. 2021\)](#), 29 June 2021.

150 Christian Perez, *Foreign Policy*, [Why China's new Data Security Law is a warning for the future of data governance](#), 28 January 2022.

cooperate with relevant authorities to address issues of national security and criminality. By not defining these terms, the Chinese state retains authority to compel cooperation from network operators handling data traffic within China. Furthermore, both laws include strict data localisation requirements, thus further increasing Beijing's control over and access to personal and corporate data. These measures represent complex challenges for the Netherlands and the EU with regards to DOSA. While efforts to re-shore critical industries continue apace, the Dutch and European economies cannot decouple from China, meaning that it is imperative to navigate these strict regulations, especially for digital and technology firms.

However, as noted previously, China also devotes resources to Shape actions in addition to its Regulate activities. Beyond the well-known Belt and Road Initiative, Digital Silk Road and Digital China initiatives discussed above, Beijing's China Standards 2035 strategy seeks to ensure that the next generation of global technology standards reflects Chinese interests.¹⁵¹ Setting standards in key fields such as next-generation telecommunications and AI will not only shape the digital landscape for decades to come, but could also hold massive implications for international trade and cooperation. If safe, human-centred standards for digital technologies cannot be agreed upon at a global level, interoperability could be sacrificed in the name of OSA.

Another relevant Shape activity undertaken by the Chinese government is the annual World Internet Conference (WIC). Held annually in Whuzhen, the WIC seeks to engage other countries to promote digitalisation, engage in dialogue on various digital matters, and promote a Chinese vision of uses and standards for internet technologies.¹⁵² Similarly, the Global Data Security Initiative, introduced in 2020, seeks to create a global framework for addressing issues in data storage and digital commerce.¹⁵³ Notably, China has since made efforts to promote this framework abroad, with Russia, Tanzania, Pakistan, Ecuador, the Arab League and ASEAN countries expressing support for the initiative. The launch in November 2022 of its white paper, titled 'Jointly Build a Community with a Shared Future in Cyberspace', represents a further step in engaging

151 DigiChina (Stanford Cyber Policy Center), [Chinese involvement in international technical standards: a DigiChina forum](#), 6 December 2021.

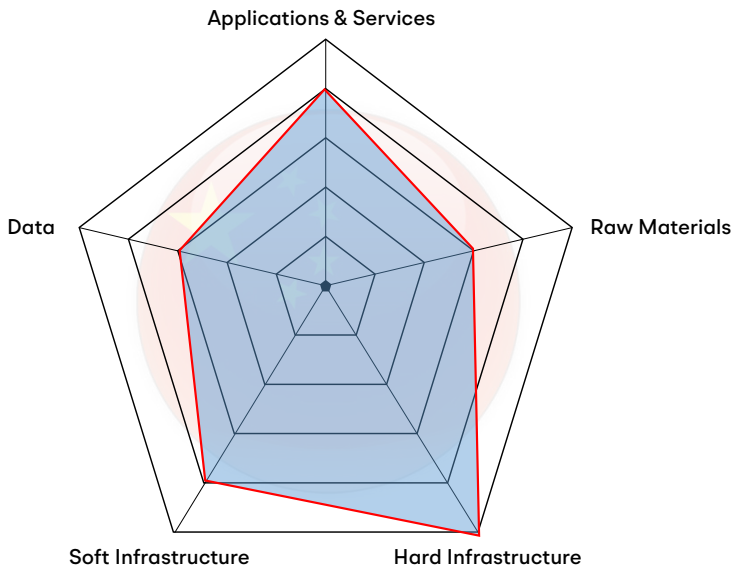
152 World Internet Conference, [Introduction to World Internet Conference](#), 22 September 2022.

153 DigiChina (Stanford Cyber Policy Center), [Knowledge base: China's 'Global Data Security Initiative'](#), 31 March 2022.

other countries on China's vision of internet development and governance.¹⁵⁴ Such actions should be carefully monitored, as their success could result in a bifurcated global digital landscape with limited to non-existent interoperability.

Figure 15 presents a radar chart to illustrate China's relative investment in the five DTS layers.

Figure 15 China's DTS profile



Source: authors' compilation.

The policies and initiatives outlined above represent a small fraction of China's engagement in the digital domain. Indeed, the full scope of China's efforts to secure digital autonomy exceed the capacity of this brief case study. For example, China is the leading exporter of rare-earth metals, a vital input for a number of digital enabling technologies. The steps taken by the Chinese government to control carefully this industry (and the implications these efforts have for other countries' digital and green transitions) is just one of many policy

154 China Daily, [Full text: 'Jointly Build a Community with a Shared Future in Cyberspace'](#), 7 November 2022.

areas relevant to Dutch DOSA. Similarly, China’s efforts to adopt widespread usage of open-source software could allow it to prevent critical software dependencies. Further study of China’s efforts could yield additional insights and allow Dutch policymakers to calibrate better the Netherlands’ DOSA approach.

3.4.3 India

As one of the world’s fastest growing developing economies, India’s approach to the digital dimension of strategic autonomy is intrinsically linked to its development goals. Accordingly, while New Delhi continues to pursue several policies under the Protect line of action, notably data localisation, its expansive portfolio of Promote initiatives reflects an intense focus on broad-based digitalisation across the Indian economy and society. Additionally, India also appears increasingly intent on assuming a leadership position among its peers in the Global South, especially on matters of technology and digitalisation. This translates into a number of efforts to Shape the digital landscape beyond its own borders, especially through its India Stack digitalisation framework. Furthermore, India’s ever increasing significance in the Indo-Pacific region and its complicated relationship with China require careful consideration. Table 10 below provides a concise overview of notable measures implemented using the PS–RP and DTS frameworks.

Table 10 Case study of India: PS–RP and DTS analysis of digital and technology policies

DTS Layers	Promote and Shape (PS)	Regulate and Protect (RP)
Applications & Services	<ul style="list-style-type: none"> Digital India India Stack ^{SR} National Policy on Software Products 2019 National Strategy for Artificial Intelligence 	<ul style="list-style-type: none"> National Cybersecurity Policy ^{SR}
Data	<ul style="list-style-type: none"> Digital Personal Data Protection Bill, 2022 (proposed) ^{SR} National Strategy for Artificial Intelligence 	<ul style="list-style-type: none"> Information Technology Act 2000 ^{SR} Information Technology Rules 2011 ^{SR} Digital Personal Data Protection Bill, 2022 (proposed) ^{SR} India Stack National Strategy for Artificial Intelligence National Cybersecurity Policy ^{SR}

DTS Layers	Promote and Shape (PS)	Regulate and Protect (RP)
Soft Infra-structure	<ul style="list-style-type: none"> • Digital India • India Stack ^{SR} • Policy on Adoption of Open-Source Software for Government of India • National Policy on Software Products 2019 • National Strategy for Artificial Intelligence • National Cybersecurity Policy 	<ul style="list-style-type: none"> • National Cybersecurity Policy ^{SR}
Hard Infra-structure	<ul style="list-style-type: none"> • Digital India • National Policy on Electronics 2019 ^{SR} • Make In India • Production-Linked Incentives (PLI) Scheme • Scheme for Promotion of Manufacturing of Electronic Components and Semiconductors (SPECS) • Modified Electronics Manufacturing Clusters Scheme (EMC 2.0) • Telecom Technology Development Fund (TTDF) Scheme • BharatNet Project • National Mission on Quantum Technologies and Applications • National e-Governance Plan 	<ul style="list-style-type: none"> • National Cybersecurity Policy ^{SR}
Raw Materials		

Note: SR refers to Shape and Regulate initiatives.

Source: authors' compilation.

Two key policy initiatives relevant to DOSA are the ‘Digital India’ and ‘Make In India’. Digital India, launched in July 2015, seeks to consolidate digitalisation efforts and focuses on digital infrastructure, digital (government) services and ‘digital empowerment’.¹⁵⁵ Make In India, which launched in September 2014, aims to increase India’s manufacturing capacity across 25 sectors,

¹⁵⁵ India’s Ministry of Economics and Information Technology – Common Services Centre, [Digital India](#).

including Electronic Systems, Information Technology (IT) and Business Process Management (BPM).¹⁵⁶

In this way, Make In India seeks not only to promote investment in the technological and digital domains, but also to offer India as an alternative to China in the world's value chains. This is apparent in several programmes under the Make In India banner, such as those for the Electronic Systems sector. These include the Production-Linked Incentives (PLI) Scheme, the Scheme for Promotion of Manufacturing of Electronic Components and Semiconductors (SPECS) and the Modified Electronics Manufacturing Clusters Scheme (EMC 2.0). Each of these arrangements provides financial incentives to domestic and foreign companies commensurate with their sales of goods manufactured in India, with a goal of rapidly increasing India's manufacturing base.¹⁵⁷ Digital India and Make In India represent significant Promote actions across the Applications & Services, Soft Infrastructure and Hard Infrastructure layers of the DTS. These policy initiatives also highlight the Indian view of electronics hardware manufacturing as a strategic imperative linked to its national security.¹⁵⁸ To this end, the National Policy on Electronics 2019 seeks to promote India's Electronic Systems Design and Manufacturing (ESDM) sector further through a combination of manufacturing targets, incentive programmes and measures to foster innovation.

India's enthusiastic Promote agenda can also be seen clearly in the India Stack initiative.¹⁵⁹ Introduced by India's government in 2009, India Stack is an online infrastructure that offers India's vast population access to finance and government services, thereby contributing to digital social inclusion. Comprised of a collection of application programming interfaces (APIs), India Stack provides software developers with direct access to a variety of government data sources

156 Make In India, [Make In India – sectors](#).

157 Make In India, [Schemes for electronics manufacturing in India](#).

158 India's Ministry of Electronics and Information Technology, [National Policy on Electronics 2019 \(NPE 2019\)](#), 25 February 2019, p. 16.

159 While this initiative utilises a Stack model, it does not represent a national technology stack or Indian DTS as described in section 3.1. Furthermore, the Data layer of the India Stack should not be equated with the Data layer of the DTS.

and digital infrastructure.¹⁶⁰ This initiative has resulted in near universal e-identity adoption across India's adult population and, more importantly, created a massive user base for a nationwide digital ecosystem that can attract firms active in the technological and digital domains.¹⁶¹ As such, New Delhi's creation of these public tools for use by private-sector actors represents a hugely successful investment in both the Applications & Services and Soft Infrastructure layers of the DTS. Furthermore, India Stack represents a strong push to *shape* the digital domain, with Prime Minister Narendra Modi's government actively *promoting* its approach as an alternative digitalisation model for developing countries around the world.¹⁶² These efforts also complement the Indian Ministry of Electronics and Information Technology's preference for Free and Open-Source Software (FOSS). Projects¹⁶³ such as the National Resource Centre for Free and Open-Source Software (NRCFOSS) and the creation of Bharat Operating System Solutions (BOSS GNU/Linux) – an open-source Linux operating system designed by the Centre for Development of Advanced Computing (C-DAC)¹⁶⁴ – are indicative of the Indian government's competences in this area.

Additionally, India Stack's Data layer represents efforts to Regulate and Protect, in line with the government's approach to data as a key enabler for economic development, and notwithstanding trade-offs with individual privacy.¹⁶⁵ India's most significant action in this arena remains its ongoing efforts to adopt new national data-protection legislation, with the most recent proposal released in November 2022. While debate continues over its draft text, it represents a marked evolution from a prior 2019 iteration, specifically in its approach to cross-

160 [India Stack](#). The India Stack consists of three sequential layers: (1) [the Identity layer](#), which consists of a variety of 'digital identity products' utilising India's Aadhaar e-identity system, such as electronic authentication and Know Your Customer ('KYC') services; (2) [the Payments layer](#), centred on India's homegrown digital payments system, the United Payments Interface ('UPI'); and (3) [the Data layer](#), which seeks to operationalise India's Data Empowerment and Protection Architecture ('DEPA') through legislation, standardisation of informed consent processes related to data collection and use, and the creation of entities that can facilitate data-sharing and consumption.

161 *Financial Times*, [The India Stack: opening the digital marketplace to the masses](#), 19 April 2023.

162 India Stack, [India Stack Global](#).

163 India's Ministry of Electronics and Information Technology, [R&D in information technology – projects](#).

164 BOSS Linux, [About CDAC Chennai](#).

165 Observer Research Foundation, [Micro matters: using data for development in the era of the fourth Industrial Revolution](#), 3 March 2023.

border data flows and data localisation.¹⁶⁶ Under the proposed legislation, cross-border data transfers to third countries may occur following a government assessment and notification process, although the text does not elaborate on selection criteria for these ‘white-listed’ countries that become ‘trusted geographies’.¹⁶⁷ Combined with the elimination of data localisation requirements, this modified approach appears aimed at satisfying the interests of both Big Tech firms and Indian companies, both of which stand to benefit from reduced barriers to data flows.¹⁶⁸ After all, if adopted, these measures could further incentivise New Delhi’s digital partners to invest in India. Additionally, while the 2022 draft represents a two-thirds reduction in content over the 2019 version, it retains individual data-protection *regulations*, outlines the rights and responsibilities of data principals and data fiduciaries, and proposes a Data Protection Board to serve as the primary data regulator in India. While clearly drawing on the EU’s GDPR for inspiration, the legislation opts for a less-prescriptive approach that focuses on establishing principles that will guide subsequent legislation and *regulations*.¹⁶⁹ Furthermore, India’s concessions do not diminish its concerns over the transfer of its national data to the world’s leading technology firms.¹⁷⁰ Nonetheless, the proposed legislation represents a combination of Promote and Protect actions, with the Indian government seeking to strike a balance between safeguarding data on a national scale and aligning itself sufficiently with partner countries to facilitate future digital cooperation.

Another key Protect measure is the National Cybersecurity Policy, adopted in 2013. This policy cuts across the Applications & Services, Data, Hard Infrastructure and Soft Infrastructure layers of the Stack and identifies India’s key strategies to secure its digital domain.¹⁷¹ In addition to conventional elements of cybersecurity, the policy also includes specific provisions for ‘Information sharing and cooperation’ and ‘Reducing supply chain risks’, demonstrating

166 French Institute of International Relations, [The technology policies of digital middle powers](#), February 2023, p. 29.

167 India’s Ministry of Electronics and Information Technology, [The Digital Personal Data Protection Bill, 2022](#), p. 15.

168 Institute of South Asian Studies, National University of Singapore, [Decoding India’s 2022 Data Protection Bill](#), 23 November 2022.

169 Data Guidance, [India: Comparing the Digital Personal Data Protection Bill, 2022 and the GDPR](#), January 2023.

170 Institute of South Asian Studies, National University of Singapore, [India and the EU’s Digital Indo-Pacific Strategy](#), 23 December 2022.

171 India’s Ministry of Electronics and Information Technology, [National Cybersecurity Policy 2013](#).

a holistic approach to this topic. However, given India's rapid digitalisation progress since 2013, New Delhi is in the process of formulating a new national strategy that better reflects the cybersecurity developments of the last decade. To this end, the Netherlands may have an opportunity to partner with India and help to *shape* its policy development. While New Delhi will define its own needs and goals in this field, the Netherlands can remain actively engaged to ensure that interoperability and cooperation remain possible. Furthermore, by prioritising these objectives, the EU can reduce barriers to potential digital partnerships that would otherwise be impossible based on a strict insistence on regulatory convergence between the two regimes.

Interestingly, India does not appear to have an explicit policy for its Resource layer, as it relates to the DTS. While India has a number of initiatives in the mining sector under the Make In India banner, these tend to focus on coal mining and improving the sustainability of mine operations.¹⁷²

However, as mentioned previously, India's efforts in the digital domain also include an international Shape component. During its presidency of the G20 in 2023, India has placed an emphasis on technology and digital matters. Specifically, Prime Minister Modi has used the presidency to emphasise the 'Data for Development' concept, making the first side event of the Development Working Group a discussion of this topic.¹⁷³ India's success in deploying data-driven solutions to its various development challenges represents a valuable 'export', as it can market these programmes to its peers in the Global South. These efforts to *shape* the use of data and digital products in the developing world represents a critical priority for India, one which it will continue to pursue even after the end of its current G20 term. Such efforts have already borne fruit, as evidenced by the successful linkage of India's Unified Payments Interface (UPI) with Singapore's PayNow system in February 2023.¹⁷⁴ The successful interoperability of this key India Stack component serves as an important proof of concept, demonstrating the possibilities of exporting its digital infrastructure to other developing countries. In this regard, India's *shape* activities are emblematic of the intertwined nature of its digital autonomy and development agendas.

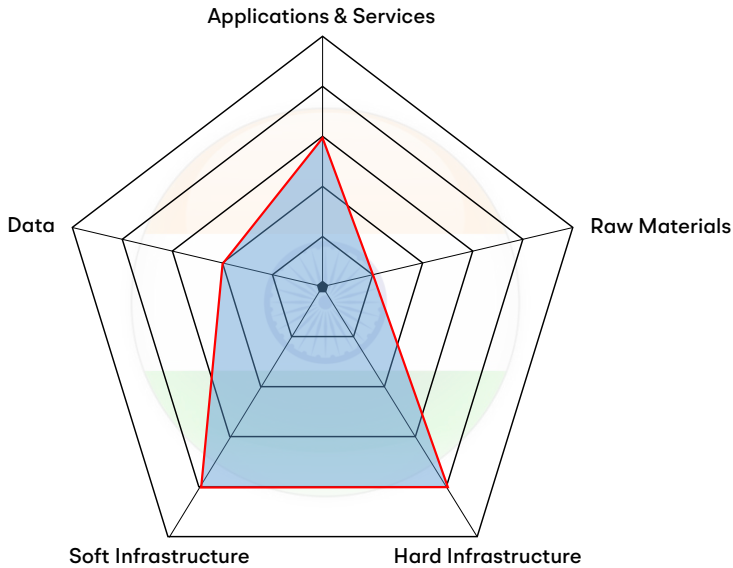
172 Make In India, [Sectors – mining](#).

173 Observer Research Foundation, [India will prioritise data for development at G20](#), 14 December 2022.

174 TechCrunch, [India and Singapore link UPI and PayNow in cross-border payments push](#), 21 February 2023.

Figure 16 presents a radar chart to illustrate the India's relative investment in the five DTS layers.

Figure 16 India's DTS profile



Source: authors' compilation.

3.5 Concluding remarks

These case studies of significant EU member states and important third countries provide a broad view of different approaches being taken to secure the digital component of OSA. All of the countries surveyed in these analyses make heavy investments in cybersecurity, with all six adopting national Protect strategies to ensure their safety in the digital realm. Furthermore, all countries reviewed are making investments in future technologies, with quantum technologies standing out as a particularly relevant example. This will be one of, if not the, most important digital-enabling technologies in the coming decades, thus warranting its universal inclusion in these countries' digital autonomy approaches. This analysis also shows how France and Germany, which lag relatively further behind in their technological or digital capabilities based on the quick scan results, have placed a stronger emphasis on the Promote line of action in recent

years. Through the use of a variety of financial incentives and investment programmes, these countries hope to nurture innovation, research, development and entrepreneurship. Additionally, the Shape line of action appears to be particularly important to the majority of these countries, with many attempting to export their models for addressing various digital matters. Another striking finding from the case studies is that most have paid remarkably little attention to the Raw Materials layer, until recently. Policies and initiatives in this layer are lacking or are rather recent in nature.

These findings and more will be discussed in the following section on actionable steps that the Netherlands can take to foster open strategic autonomy in the digital domain.

4 Towards digital resilience and autonomous choices: actionable steps

The European Economic Security Strategy, launched by European Commission President Ursula von der Leyen in June 2023, is a milestone, advocating for a much tougher stance in the context of increased geopolitical tensions and accelerated technological shifts. The strategy introduces a Promoting–Protecting–Partnering approach to mitigate the risks associated with these tensions and shifts, highlighting the importance of building partnerships with reliable countries that are invested in contributing to the same overarching objectives as the European Union. This aligns the EU more closely with the Dutch mindset, reflected in the PS–RP framework that has steered the Netherlands’ DOSA-related efforts (see Figure 4 above and Figure 17 below).

While the strategy includes significant Protect instruments, concrete steps on Promote measures remain elusive. The strategy focuses on ‘minimising risks arising from certain economic flows, while preserving maximum levels of economic openness and dynamism’¹⁷⁵ risks to the resilience of supply chains, including energy security; risks to the physical and cybersecurity of critical infrastructure; risks related to technology security and technology leakage; and risks of economic coercion through the weaponisation of trade dependencies. Strengthening the strategy’s digital elements is important, and may be achieved by steering attention to the risks that new (digital) technologies may pose to fundamental rights such as the right to non-discrimination, freedom of expression, human dignity, personal data protection and privacy. It details instruments such as inbound and outbound investment screening, as well as export controls on high-tech and sensitive areas including quantum computing, artificial intelligence and advanced semiconductors.¹⁷⁶

175 European Commission, [An EU approach to enhance economic security](#), 20 June 2023.

176 Politico, [EU looks to ban companies from making sensitive tech in China](#), 20 June 2023.

Figure 17 Promoting–Protecting–Partnering framework, introduced in the European Economic Security Strategy



Source: European Economic Security Strategy Factsheet. See [European Commission, An EU approach to enhance economic security, 20 June 2023](#).

Strikingly, 'open strategic autonomy' is mentioned just once in the 14-page European Economic Security Strategy. As the EU moves in this new direction, the Dutch government should consider reformulating its current DOSA narrative in terms of digital economic security (DES). Engagement with the European Economic Security Strategy and embracing the notion of DES will help to focus energy and attention on action, rather than rhetorical discord, and enable the Netherlands to leverage its reputation as a European frontrunner in the geopolitics of technology and digitalisation to achieve a balanced approach.

Set against this context, and drawing from the policy shifts and case studies presented in earlier sections of this report, this final section: 1) summarises good practices of other countries; and 2) proposes actionable steps for the Netherlands and the EU to work – with partners abroad and in the private sector – towards the implementation of open strategic autonomy in the digital domain.

4.1 The Netherlands as an EU member state

- **Share Dutch best practices (Shape).** Using its networks of attachés responsible for Innovation, Economic Security, Cyber and Knowledge at Dutch embassies worldwide, the Netherlands can proactively share its best practices with the EU and other member states to shape their course.
- **Do not run alone; be mindful of other member states.** Invest in an inclusive approach on issues where the Netherlands has a unique position, such as export controls on semiconductor equipment, to increase the likelihood of getting them on board in a desirable direction.
- **Engage with the industrial policy practices of France and Germany.** Engaging with German and French willingness to support industrial policies that nurture the growth of high-tech and digital firms can help attract investments and entrepreneurship to EU member states.
- **Learn from Finland's long-standing public-private cooperation on security of supply.** The Finnish approach of voluntary, structural and mutually beneficial public-private cooperation to ensure the security of supply holds important lessons for the Netherlands to engage the private sector.

Recent years have seen a reversal of the more critical and restrained Dutch policies towards the EU that emerged in the mid-2000s. The understanding that the Netherlands needs the scale of a European shield and sword to cope with the current geopolitical and technological environment has led to a reappraisal of the EU – at least among Dutch elites. The Dutch Policy Note on China of 2019 – the first among EU member states and a milestone in the shift towards a more critical stance – followed by its push, together with France and Germany, for an Indo-Pacific strategy illustrate this. Having lost a key EU ally because of Brexit, the Netherlands also sought to reinvent its partnerships with other big EU member states, particularly France. The Netherlands' adoption of new export controls and participation in European IPCEIs evince the turn towards a more French mercantilist mindset. Yet, importantly, the Dutch cooperated with Spain to navigate France's push for EU strategic autonomy towards 'open strategic autonomy' – highlighting the need to preserve maximum levels of economic openness and dynamism.

Paralleling investments in Economic Security Attachés and Cyber Attachés at Dutch embassies worldwide, the Netherlands has invested in Dutch eyes and voices in EU institutions of relevance to the geopolitics of technology and digitalisation.¹⁷⁷ Yet such engagement with the EU's Promote agenda seems to be lagging; the Dutch have no commissioned official in the Directorate-General for International Partnerships' (DG INTPA) Digital for Development (D4D) Hub.

4.1.1 The Netherlands as seen by other EU member states

The Netherlands is seen by other member states – and appreciated by more than a few officials in Brussels – as a flagbearer of open markets and free trade, calling for proportionality and precision in new industrial policy and economic security measures. The Netherlands has actively *shaped* the creation of new instruments on specific issues and technologies, such as export controls, the economic coercion instrument and quantum technologies. At the same time, it is pushing back on – although not blocking – other fronts, including the notion of European tech champions.

This mixed approach reinforces the Netherlands' position as a European frontrunner with a sense of realism about new risks and tides, and yet a critical mindset that continues to favour openness in principle. That said, the Dutch government has been criticised for moving too readily – and without much consultation with the EU and other member states – on issues where it has a unique position – that is, on semiconductor equipment and, therefore, export controls. This will certainly impact the likelihood of other EU member states getting on board with this new direction, as the Dutch now desire. The Netherlands needs to invest more if it wishes to uphold its reputation and continue to be seen as a first-mover that can inspire other middle-sized EU member states.

This push should involve the highest political echelons. Indeed, as (digital) economic security is now considered a *Chefsache* – with Ursula von der Leyen herself pushing the agenda forward in Brussels – the silence of Dutch Prime

177 Examples include the European External Action Service (EEAS), involved with the Trade and Technology Councils, the Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW), which plays a key role in addressing concerns about economic coercion, DG CONNECT, and even Silicon Valley. In addition, representatives of the Dutch Ministry of Internal Affairs – host to the Dutch Minister for Digitalisation – have been added to the Dutch Permanent Representation in Brussels.

Minister Mark Rutte is notable. While the prime minister has spoken out on other relevant matters at the EU level, he has remained largely silent on this topic. In stark contrast, Presidents Macron of France and Modi of India are key examples of leaders who take an active role in pushing this important agenda forward. Relatedly, there is a need for new governance structures, at national and EU levels, to foster a whole-of-government approach that entices all ministers while deepening the knowledge base of officials at all levels. This necessitates a powerful EU commissioner or national minister who oversees, but does not duplicate, the Protect–Regulate and Shape–Promote actions of ministries involved with this broad agenda.

While different EU member states lead on specific sub-sets of the tech and digital agendas, the Netherlands stands out as one of only a few EU member states that are investing in critical and emerging technologies, such as semiconductors, AI, 5G/6G and quantum. In addition, its active stance on digital diplomacy and cyber diplomacy is appreciated in Brussels, including its leading role in discussions with Singapore.

On the Promote agenda, the Netherlands has more difficulty to match other EU member states, although investments are being made. Germany has an edge on implementing an international digital strategy, benefiting from having an implementation agency (the GIZ) that is present in Brussels and throughout the world. The Netherlands would benefit from having instruments and defining a niche of its own in this line of action. Denmark, for example, is looking to invest in sustainable supply chains – specifically, green shipping corridors, aiming to achieve zero-carbon shipping with a hydrogen-based fleet. As a key logistical hub, the Port of Rotterdam is one of the five European ports engaged in this project.¹⁷⁸

4.1.2 Learn from Germany’s industrial policy practices

Perhaps the greatest difference in approaches between the Netherlands and Germany remains Germany’s willingness to support industrial policies that nurture the growth of high-tech and digital firms, both nationally and at the European level. Thus, while a Dutch approach to digital economic security may not adopt similar measures, it will need to acknowledge the potential of such

178 Ministry of Foreign Affairs of Denmark, [New European Green Corridors Network with participation of the Danish Port of Rønne launched](#), 30 March 2022.

measures to attract investments and entrepreneurship to other EU member states. However, such policy divergence does not preclude cooperation. The Netherlands should increase its efforts to coordinate research and development of critical emerging technologies (such as quantum computing and 6G) across EU member states to compete better with the United States and China. Integrating digital and technological hubs such as TU Delft with Germany's 12 identified Digital Hubs could help accelerate innovation without interfering with market forces. As noted in section 3.3.1, Germany's goal of creating binding, EU-wide security standards for ICT infrastructure represents another area of potential cooperation with the Netherlands, as such regulations could improve the security and competitiveness of the Single Market. Furthermore, Dutch competences in this realm would likely provide the Netherlands with a significant opportunity to *shape* such a policy in line with its own defined best practices. Finally, given the extreme strategic importance of ASML to Dutch DOSA, the Netherlands must closely monitor German supply-chain management policies that could implicate the semiconductor supply chain.

4.1.3 Learn from France's focus on building European strengths

The Netherlands will encounter similar challenges when attempting to synchronise its digital economic security approach with France as those presented by Germany. Both of these critical EU member states prefer more direct interventions to achieve their strategic objectives, which stands at odds with Dutch preferences. Given these similarities, the Netherlands must take similar lessons from the French approach, chief of which are the potential risks and rewards of foregoing similar measures at the national level. However, France's efforts to foster domestic and European technology champions do present opportunities for building Europe's overall capacity in critical emerging technologies such as quantum computing. As these research areas represent critical opportunities from both strategic and commercial perspectives, the Netherlands should not shy away from deepening cooperation with eager member states like France and using government resources to incentivise their development. In this regard, the Netherlands should analyse the relative effectiveness of French efforts to date and adjust them to fit the Dutch national context. Additionally, France's extensive state-led development work abroad in the digital arena could serve as an additional model for building similar Dutch mechanisms. Programmes such as D4D and Global Gateway have highlighted the need for large-scale investments to meet the needs of developing partner countries, which will require a paradigm shift for the Netherlands to remain relevant in this arena. Scaling up development cooperation will help The Hague

build durable partnerships abroad that can yield benefits across all DTS layers. Such investments may create numerous opportunities for Dutch businesses in the technology and digital domains.

4.1.4 Learn from Finland's focus on security of supply

The Finnish concept of security of supply offers a rich opportunity for the Netherlands to refine its digital economic security approach, specifically on the stable and secure supply of raw materials, but also on other domains where the private sector plays a key role. A defining feature of this strategic tradition lies in the engagement between the public and private sectors, in a structured setting and largely on a voluntary basis. The success of this approach lies in the fact that companies benefit from being in a structural dialogue with government and gain a sense of what is happening around the world. The Dutch government could learn from the Finnish approach to public–private cooperation to bolster its own efforts to engage the private sector, even beyond the security of supply. This goes far beyond the Economic Security Business Desk that was established in the Netherlands in May 2023¹⁷⁹ to answer questions from companies and universities about implementing specific measures. Creating formal mechanisms to discuss new economic security measures and solicit feedback from these critical actors would improve the efficacy of Dutch efforts and create partnerships akin to those observed under the security of supply model. Additionally, identifying critical sectors where statutory requirements for risk mitigation could be deployed would further strengthen the Netherlands' Protect position. Improving Dutch understanding of the Finnish approach will be crucial for future coordination as economic security grows in criticality to both the Netherlands and the EU. The Netherlands could also leverage its strength in the areas of cybersecurity and standards to deepen coordination with Finland on Protect measures in these areas. Finally, Finland's efforts to invest in digital-enabling infrastructure to accelerate innovation should be leveraged to complement Dutch efforts to develop critical technologies such as advanced batteries and quantum computing.

179 BNR Nieuwsradio, [Ondernemersloket Economische Veiligheid als middel tegen spionage](#), 31 May 2023 (in Dutch).

4.2 Cooperating and dealing with third countries

- **Multilateralism where possible, minilateralism where needed. Aim to keep dialogue and consensus at the highest level possible.** For strategic themes, engage in sectoral minilateral settings to enable focused collaboration with like-minded partners.
- **Pick your partners.** Co-create with ‘Digital Partners’, communicate with ‘Friendly Competitors’ and captivate ‘Potential Converts’ and ‘Analogue Challengers’.
- **Involve the private sector and civil society.** Act on the understanding that, ultimately, it is European companies – large and small – and citizens that will feel the consequences of the new economic security agenda.
- **Learn from the US’s targeted cooperation on tech and digital in minilateral settings.** EU and Dutch strategic cooperation on technology and digital issues with third countries should be taken beyond bilaterals towards sectoral and minilateral cooperation with key countries.
- **Learn from China’s Shape approach.** Delivering on digital projects of substantial scale and impact are requirements to raise the Dutch and EU’s international profile and credibility with partner countries in the Global South. Leverage expertise in areas like cybersecurity to create new international standards in this domain that reflect European values.
- **Learn from the India Stack initiative.** Dutch and European tech and digital firms should investigate how to benefit from the India Stack initiative, both as a best practice to implement at home as well as a basis to access the biggest market in the world.

Successful de-risking in the digital domain cannot be achieved by the EU – let alone, the Netherlands – itself. Engagement with other countries in bilateral and multilateral settings must be targeted on specific sectors and topics, and complemented with minilaterals when necessary. Lessons can also be drawn from key partners, especially the United States, China and India.

4.2.1 Multilateralism where possible, minilateralism where needed

The shift from multilateralism to minilateralism is an important factor for Dutch and European authorities to consider when formulating DOSA-oriented policy. Remarkably, except for the G7 and G20, the tech and digital partnerships in which the EU is engaged – that is, the DPAs and the TTCs – are bilateral (see section 1.3). Although these are certainly relevant, the Netherlands and the EU should consider supplementing this approach with strategic, sectoral, minilateral arrangements. Critical areas of economic security concern, such as supply-chain security, semiconductors, advanced computing, artificial intelligence and biotechnology, would benefit from sectoral partnerships with like-minded countries and reduce duplication of efforts across a web of bilateral arrangements. Settings like the Chips 4 Alliance and SCRI should be closely monitored in order to understand how such collaborations might bring benefits to the parties involved (see section 1.3.2). However, the disadvantages of the current shift from multilateralism to minilateralism should not be overlooked. First, minilateralism implies, by definition, less consensus and buy-in. In some contemporary tech-related challenges – such as the spread of standards, technical or otherwise – minilateralism reduces the global impact that certain agreements could have. Additionally, officials point out that the coordination effort to manage and align multiple dialogue platforms is often underestimated. The mantra should hence be ‘multilateralism where possible, minilateralism where needed’.

Second, in a time of ‘de-risking’ and ‘trusted supply chains’, partnering with others can be a way to avoid potentially more costly Protect measures that also limit market openness and trade opportunities. First and foremost, partnering is about fostering mutually beneficial relationships with like-minded countries that not only share digital and technological capabilities, but also interests, concerns and/or principles (‘Digital Partners’, see section 3.2.3). These countries will play a crucial role in co-creating and pushing the DES agenda forward over the coming years in all DTS layers, together with the Netherlands and the EU. Moreover, nurturing meaningful relationships and keeping open communication channels with technologically and digitally advanced countries that may occasionally have divergent interests, or that compete with the Dutch and/or EU in specific areas (‘Friendly Competitors’), will also be increasingly relevant. A case in point is the Dutch–Japanese shared need to manage US pressure for export controls on lithography machinery to China. Finally, engaging to some extent with ‘Potential Converts’ and ‘Analogue Challengers’ should not be discarded. While countries that fall into these categories may not be significantly

influenced by Dutch and European policy-making, it is advantageous to try to captivate them. This can be done by presenting them with an alternative to China's autocratic and state-capitalist approach. Ultimately, these countries also have expanding digital economies and markets that Dutch and European companies should consider.

4.2.2 Learn from the US's targeted development cooperation

With the size of its economy and broad strengths across digital and technological domains, the United States possesses greater capacity to pursue its digital autonomy agenda unilaterally than the Netherlands, especially in the Protect line of action. As such, while the Netherlands may join in US efforts, such as recent cooperation in implementing Washington's export control regime for the semiconductor sector, it cannot necessarily replicate them. However, because US policy can have wide-reaching implications for both the public and private sectors, the Netherlands should prioritise building upon this bilateral cooperation to remain informed of the United States' evolving strategy. To this end, the EU-US TTC (see section 1.3.1) has increasingly functioned as a forum for both blocs to establish an open dialogue and align on industrial policy measures, and its scope has been extended to include more themes that fall under the notion of economic security. Examples of this are the ongoing talks on export controls and non-market practices, as well as the recent establishment of a joint task force working on quantum technologies.¹⁸⁰ It is important for Dutch diplomacy to have wide communication channels and mechanisms to shape the developments of the EU-US TTC. Furthermore, the EU should ensure cohesion between the transatlantic TTC and similar channels with other key allies – such as the DPAs with Japan, South Korea and Singapore, the EU-India TTC, the G7 and other minilateral (sectoral) settings. Additionally, the US strategy of engaging in targeted development cooperation to achieve mutually beneficial outcomes could be replicated by the Netherlands. Such an approach will require a paradigm shift, as it would de-emphasise the typical Dutch open-market orientation in favour of strategic investments. However, such expenditures could yield significant benefits, such as improved access to critical raw materials, new markets for Dutch goods and services, and opportunities to test emerging technologies.

180 European Commission, [Joint Statement EU-US Trade and Technology Council of 31 May 2023 in Lulea, Sweden](#), 31 May 2023.

4.2.3 Learn from China's Shape approach

The Netherlands should take heed of China's various Shape initiatives, as these efforts represent a clear attempt to project Chinese influence into the digital domain. Indeed, beyond projects that fall under the banner of the Digital Silk Road initiative, China Standards 2035 and the Global Data Security Initiative are but two of many such examples. While the Netherlands should not seek conflict with China, its strong digital profile and expertise could allow it to inform a European alternative to these Shape efforts on the international stage. For example, Dutch strength in the cybersecurity domain could be leveraged to create new international standards in this field that reflect European values. Additionally, increasing Dutch engagement with the D4D initiatives and Global Gateway could raise the Netherlands' international profile and credibility with partner countries in the Global South. As an alternative to China's Belt and Road and Digital Silk Road initiatives, these programmes create opportunities to build new partnerships that could enhance Dutch and European Shape efforts. However, the Netherlands should as much as possible continue to engage China in this process to prevent further bifurcation of the world's digital landscape. Finally, as economic security discussions continue in Brussels, in order to avoid potential future coercion, the Netherlands should review its exposure to China in its critical supply chains, as in the case of Lithuania in 2021.¹⁸¹ The Netherlands has already exposed itself through the imposition of export controls on exports of semiconductor manufacturing equipment, so such a review is imperative.

4.2.4 Learn from the India Stack initiative

The Netherlands could benefit greatly by contributing to the rapidly expanding ties between the EU and India. While the EU–India TTC represents perhaps the clearest example of efforts to increase engagement with this key Indo-Pacific country, the Netherlands could also deepen its bilateral ties to the world's most populous nation. India's rapidly advancing digital ecosystem under the India Stack initiative could serve as an excellent new market for Dutch digital and technology firms, providing a massive consumer base for their goods and services. Additionally, European and Indian preferences for open-source development practices offers many opportunities for collaboration. While India already hosts IAs and ESAs, creating new mechanisms to connect the business communities and civil societies of both countries could further encourage

181 Center for Strategic and International Studies, [China's economic coercion: lessons from Lithuania](#), 6 May 2022.

mutually beneficial, market-driven exchanges. Such engagement could also improve interoperability of the Dutch and Indian digital ecosystems, which could in turn make the creation of an EU–India Digital Partnership Agreement easier to achieve, especially in conjunction with India’s forthcoming Digital Personal Data Protection Bill. Further cooperation could also be achieved in the realm of strategic technologies, whereby both sides could help the other to improve their own strategic autonomy, and cybersecurity, as India is in the process of reevaluating its current legislative framework in this critical digital area. Finally, although not directly related to the digital domain, the Netherlands could consider supporting New Delhi’s use of the ‘Global South’ moniker and its efforts to serve as the voice for this diverse collection of developing countries. Doing so could not only improve the Netherlands’ ties with India, but also improve the EU’s ability to engage with other key developing countries on topics relevant to various DTS layers, such as Raw Materials, Infrastructure and Data.

4.3 In focus: Promote

→ **Promote at home.** *The turn to smart industrial policy is certain but painful. To continue to be seen as a constructive engager, the Dutch government can focus on structural reforms that enable a thriving digital ecosystem, as well as on ensuring a market for investments by engaging end-users in investment programmes.*

→ **Promote and Shape abroad.** *Concrete steps are still lagging, especially when compared to the rapid adoption of Protect instruments. The Netherlands and the EU thereby risk losing important allies that are needed for success in DOSA: the private sector and emerging economies.*

Technological leadership, fostered by talent and sustained by (digital) technology champions, as well as convergence on digital rights and principles with a significant group of developing countries, are key aims of the Promote line of action. Technological strength attracts investments, while European private-sector investments abroad encourage the adoption of European standards and principles. Both are crucial to strengthening Europe’s position. Although initial steps in these directions are hesitantly being made in the Netherlands and in an EU context, much more must be done.

4.3.1 Promote at home: industrial policy and innovation

Notwithstanding its aversion to government involvement in the economy, the Netherlands has invested in the Promote agenda at home at crucial moments in history. The company that grew to be ASML received state support when it most needed it – back in the 1980s – and the Dutch government is now investing greatly in a digital ecosystem for research and development of quantum technologies, under the flag of Quantum Delta NL. Germany and France are heavily investing in quantum as well (see sections 3.3.1 and 3.3.2) – as well as a handful of other European countries – and these efforts need to be fully synchronised in order to compete with the United States and China. Particularly as the EU is bolstering its Protect measures, such as new screening mechanisms, care needs to be taken also to *shape* an environment that enables investment – including from non-European trusted geographies – in these new technologies.

In recent years, the Netherlands and the EU have been turning towards ‘smart(er) industrial policy’ that focuses not on support to traditional industries, but on highly innovative industries and sectors that play a key role in the green and digital transitions.¹⁸² Here, inspiration can be drawn from Japan’s creation of Rapidus,¹⁸³ which is unique in incorporating end-users (of next-generation semiconductors) in the chip-building consortium in an attempt to ensure that a market exists for innovation investments. This sets it apart from the European CHIPS Act. Propagating an end-use-driven approach – and similar best practices – also in the EU will ensure that the Netherlands is not seen as merely opposing the new trend, but instead as a constructive partner in ensuring the proportionality and precision of new measures.

Such constructive engagement and investment in a digital ecosystem that supports not just research and innovation, but also commercialisation, is also needed in other areas. The Netherlands chose not to join the European Tech Champions Initiative, launched in February 2023 to help promising EU start-ups stay in Europe.¹⁸⁴ The Dutch aversion to adding cash to private-equity funds that in turn are expected to fund promising start-ups on the verge of becoming big companies is known. However, steps of this sort – with other examples being the European Sovereignty Fund and the European Innovation Council’s EIC Scale Up

182 Adviesraad Internationale Vraagstukken, [Slimme Industriepolitiek: een opdracht voor Nederland in de EU](#), 18 March 2023 (in Dutch).

183 Nikkei, [Japan chip venture Rapidus aims for 2-nm prototype line by 2025](#), 25 January 2023.

184 European Investment Bank, [European Tech Champions Initiative](#).

100 Initiative¹⁸⁵ – may be hard to avoid in an international setting where US and Asian investors readily snatch up promising new companies. The real solution to Europe’s problems requires reform in broader policy areas – such as access to languages, visa policy, labour systems, banking and education. In the interim, however, funds like this may be a necessary short-term evil. They should also be seen as balancing the negative effects of Protect measures – such as more comprehensive investment screening, including the Dutch ‘Vifo Act’ (see section 2.2) – that add obstacles for aspiring European champions to access (foreign) funding.

4.3.2 Promote and Shape abroad: new instruments to act on local needs

The Netherlands has been active in trying to Promote and Shape. The varied networks of Dutch attachés show the Dutch government’s willingness to have local presence and be close to where the needs and opportunities are (see section 2.2.1). The Connectivity Envoy and Indo-Pacific Envoy at the Dutch Ministry of Foreign Affairs’ headquarters in The Hague further illustrate this point. However, concrete results and knowledge-gathering are still lacking. A key reason for this seems to be the lack of a toolbox – in particular, trusted relationships with the private sector and instruments. For example, the EU and Dutch government officials need a better understanding of the limits and constraints of the private sector, and of where bidding for large infrastructure projects – such as 5G or submarine cable projects – takes place, what the local challenges are (for example, the regulatory framework), and where there is an interest to work with Europeans. Furthermore, new financial instruments such as the European Fund for Sustainable Development Plus (EFSD+) and European export credits (now under discussion) can enable the private sector to de-risk in less developed environments and deliver on the scale of the hard digital infrastructure investments that are sought by emerging economies.

A second reason that explains why implementation of Shape efforts abroad is lagging is the lack of understanding of the real needs of emerging economies. As one EU official put it, ‘the European Union is good in identifying its own priorities, but not as much in identifying needs [of third countries]’. Along with the

185 Reuters, [EU looks to 100 unicorns to boost green, digital goals](#), 1 June 2023; and European Commission, [A European Sovereignty Fund for an industry ‘Made in Europe’ | blog of Commissioner Thierry Breton](#), 15 September 2022.

top-down geopolitical cooperation in the TTCs and DPAs, what the EU – and the Netherlands specifically – needs now is a growing presence and action on the ground, and professionals with knowledge of the financial instruments that are required to implement large-scale projects. These people may be deployed at representations abroad or, better, at local development and investment banks, as well as development agencies. Doing so will ensure that the European Union and its member states have the necessary intelligence and are better equipped to respond with concrete projects and initiatives within current and future frameworks, such as Global Gateway and D4D.

The EU does not yet have a database of European tech and digital strengths and local needs – let alone of matches between the two – and those should be a focus in the short term. This adds further urgency to the call for trusted relationships and closer cooperation with the European private sector and business representatives. Companies often not only have privileged access to business data, but they are also ultimately responsible for – and interested in – supporting the private sector in third countries. New financial instruments can incentivise them to pursue opportunities in countries that are of particular foreign-policy relevance to the EU, as the EU pursues its own economic security. After all, as noted in section 1.3.1, European companies are a most practical way to bring human-centred digital principles and standards, which are embedded in their business operations, to third countries.

As such, large-scale Global Gateway and D4D projects are a bottom-up complement to the top-down regulatory and government-to-government cooperation that the EU pursues with emerging economies. The digital economy packages that the EU agreed with Nigeria and Colombia are steps in the right direction.¹⁸⁶ As the case of Ericsson in 5G in Malaysia shows,¹⁸⁷ becoming part of the trusted vendors' network leads to good access and valuable intelligence for deepened engagement thereafter. For now, however, the Netherlands and the EU lack sufficient capacity to pursue this in a significant number of countries. Ambitions and initial steps notwithstanding, the Netherlands has been relatively

186 Delegation of the European Union to Colombia, [*The European Union launches the Digital Economy Package to strengthen its partnership with Colombia in the sector*](#), 15 March 2023; and European Commission, [*H.E. Prof. Yemi Osinbajo, Vice-President of the Federal Republic of Nigeria, and H.E. Margrethe Vestager, Executive Vice-President of the European Commission, met in Abuja on 13 February 2022*](#), 13 February 2022.

187 Ericsson, [*Media statement on Ericsson's contract to deploy 5G for Malaysia*](#), 3 March 2022.

less active in these development-oriented Shape activities outside the EU. Increasing engagement with Germany and France on these topics to build the Netherlands' development profile could facilitate the formation of mutually beneficial partnerships that could build Dutch DOSA with strengthened global outreach.

4.4 In focus: Protect

- **Protect measures are more successful if adopted by more countries.** Greater investments are needed to engage also less-like-minded countries on Protect measures. This requires more clarity on what we are able to give in and are willing to give up.
- **Diversification and back-up plans are needed in all layers of the Digital Technology Stack.** Vulnerabilities stemming from dependencies on in-depth, integral digitisation using technology that is managed and developed by foreign parties predominate. Analogue back-up plans need more attention.
- **Companies and academic institutions must be enticed to act on economic security.** New instruments are needed to develop relationships of trust between the public and private sectors.

On the Protect side, the Netherlands has invested significantly in *shaping* and adopting EU-wide and national-level instruments, as well as in trusted dialogues on cybersecurity with a variety of countries, including Indonesia and South Korea. Going forward, a key challenge will be to move beyond its comfort zone and invest in deeper cooperation – also on Protect measures – with less-like-minded partners that play an important role in other parts of the world and wish to strengthen their own economic security. This includes a diverse set of countries, such as India, Vietnam, Turkey and Brazil. Stronger engagement with these countries requires more clarity, also on what we are willing to give up and where we are able to give in. With India, for example, reconsidering long-standing export controls that impede technology transfer on no-longer-so-sensitive

products that India values might help reset the relationship to a greater focus on cooperation on strategic technologies.¹⁸⁸

Another Protect measure that needs more attention going forward is the question of whether, or to what extent, the EU and its member states have thought of back-up plans for key areas. Acting on this concern has started in the Raw Materials layer, as the Covid-19 pandemic and systemic rivalry with China alerted officials and firms to the risk of dependencies on single suppliers. This thinking should be extended to all other layers of the Stack, from Hard and Soft Infrastructure to Data and Applications. The vulnerabilities stemming from dependencies on in-depth, integral digitisation using technology that is managed and developed by foreign parties are especially relevant for a country like the Netherlands that has (all too) readily become a digital society. Such risks grow as citizens hardly carry cash – or can access cash through analogue systems – and alternatives to digital means of accessing government services are phased out for efficiency purposes. Attention to mitigating the risks and vulnerabilities associated with this appears limited, and more attention needs to be given to keeping or creating (analogue) fall-back options and alternatives. Designing such back-up plans implies a hierarchical compartmentalisation of systems. 5G networks provide such an example, where some countries allow the presence of Huawei equipment in their mobile telecommunication access networks, but not in the core network.

Last but not least, investing in trusted relationships with the private sector and civil society is also crucial for the success of the Protect side of digital economic security. The notion of OSA and the necessity of economic security measures remain unclear to the majority of businesses and universities, largely because of government inaction. While the recently opened Economic Security Business Desks have begun educating Dutch corporations and universities on their roles in this new strategy, more can and should be done. Platforms to engage with the private sector on major political decisions and to hear *its* challenges, concerns and wishes have yet to be created. This is important, as these companies and knowledge centres are the ones that must incorporate economic security into their operational management. Also, only they can help other countries with their economic security, through large-scale investments in, for example,

188 Vera Kranenburg and Maaïke Okano-Heijmans (eds), [How strategic tech cooperation can reinvigorate relations between the EU and India](#), January 2023.

stable telecommunication networks and secure data centres, so that they are not built exclusively with Chinese money and principles. The EU's Global Gateway, the G7's Partnership for Global Infrastructure Investments, and similar initiatives by partner countries like Japan and South Korea serve as a step in that direction.¹⁸⁹ Furthermore, aforementioned measures such as inbound and outbound investments, and export controls, have a direct impact on companies operating in high-tech. They should, therefore, be consulted when designing such measures, to avoid unbalanced implementation.

As a confidence-building measure, the Netherlands and EU should also consider learning from Japan, where a (bi)annual Economic Security Business Survey¹⁹⁰ has become a valuable tool to deepen officials' understanding of companies' perspective and to deepen discussions. Ultimately, such relationships of trust with the private sector should be extended also to businesses in partner countries that play a role in our economic security. Investment in trusted vendors can partially replace more costly investment in the promotion of European (digital) technology champions. Finally, European civil society must also be involved in policymaking on these themes, since it will ultimately reap the benefits, or suffer the consequences, of the current shift towards economic security. Civil society also functions as the guardian of its own values and principles, which must be safeguarded amid the ongoing political transformations and policy shifts.

4.5 Concluding remarks

In recent years the Netherlands has sought to foster debate on open strategic autonomy in the digital domain under the DOSA label, both in Europe and beyond. The Spanish Presidency of the Council of the EU, held during the second semester of 2023, placed OSA and its digital component as one of its priorities.¹⁹¹ However, the new European Economic Security Strategy suggests that OSA is slowly disappearing from the Brussels lexicon. Importantly, the new strategy incorporates many elements of DOSA – such as the need to act on Promote, Regulate and Shape (or Partner), alongside investments in Protect measures.

189 European Commission, [An EU approach to enhance economic security](#), 20 June 2023.

190 Asia Pacific Initiative, [Survey of 100 Japanese companies on economic security](#), February 2023.

191 Spanish Presidency of the Council of the European Union, [Priorities](#), July 2023.

The Netherlands would do well to ride this wave, and focus on fleshing out the details and actionable steps of digital economic security.

Each layer of the Digital Technology Stack requires measures and safeguards in the Promote and Protect lines of action, although the case studies in this report have shown that some measures are cross-cutting between layers. Clearly, this is a multi-dimensional rather than a linear system. In a digitally connected world, geographical borders lose relevance and walls are more difficult to build – let alone implement. This necessitates a shift to systems thinking, wherein governance structures facilitate linkages between the different objectives of upholding digital rights, enhancing technological leadership and ensuring that we have a choice in each layer of the Stack.

Going forward, greater investments need to be made in conversations with key stakeholders – especially the private sector, but civil-society organisations as well – on the need for, and objectives of, investing in digital economic security. Objectives have, by and large, been formulated in negative terms, focusing on what is to be avoided or mitigated rather than what is to be achieved – whether that is dealing with China as a systemic rival or harnessing the growing might of Big Tech companies. With more awareness now of the need for action, investments need to go into positive engagement and empowerment. This includes making use of the power of technologies, including open-source and decentralised approaches, to nurture and maintain a digital society that incorporates fundamental rights such as the right to non-discrimination, freedom of expression, human dignity, personal data protection and privacy. Strategic clarity about the ultimate goals and in what kind of society we want to live will help develop a clear narrative that steers policymakers in the right direction (towards implementation). It will also encourage companies to incorporate these rights and goals in their technologies, digital products and services, and will empower citizens to act on their rights from the bottom-up.