ie UNIVERSITY
CENTER FOR THE GOVERNANCE OF CHANGE

cgc.ie.edu

BEYOND LEGO

THE NEED FOR EU-BASED BUILDING BLOCKS OF TECHNOLOGY

POLICY PAPER #2
APRIL 2025

TABLE OF CONTENTS

AUTHORS:
Alexandre Ferreira Gomes
Maaike Okano-Heijmans
Jelle van den Wijngaard

Clingendael Institute

01. INTRODUCTION

The rapid adoption of digital technologies during the past decade has significantly transformed the realities of daily life, business interests and ultimately geopolitics. Countries and companies define digitalization goals and try to accommodate innovations, such as using artificial intelligence to summarize documents, while overcoming challenges brought about by technological developments, including privacy concerns. The European Union (EU), known for its regulatory-driven approach to technology and digitalisation, is certainly no exception. The goals set out by the EU in its 'Europe's Digital Decade' communication of 2021 showcase the bloc's ambition to accelerate and lead in digital transformation by working with Member States towards targets for digital adoption.[1]

The past decade has shown that technology is not a mere drive for positive change, however. As new breakthroughs emerge, technologies have become a geopolitical instrument of influence and coercion, as Russia's disinformation campaigns or cyberattacks on Ukrainian power grids demonstrate.

> Over the past half year, during the lead-up to and aftermath of the 2024 United States (US) elections, landmark publications such as Mario Draghi's[2] report on European competitiveness and the EuroStack initiative[3] have identified a myriad of hurdles and emphasized the urgency for Europe to assert its digital sovereignty.

Acting on these challenges, the EU Competitiveness Compass, launched by the European Commission in January 2025, presents a policy roadmap to support the efforts required by European industry to meet these challenges.

Set against this backdrop, this policy paper sheds light on the geopolitics of technology and digitalization, particularly in relation to the EU's position vis-à-vis the US and China. It analyzes the key building blocks that constitute the so-called technology stack, illustrated through the example of an AI chatbot. The building blocks range from critical raw materials (CRM) to knowledge and applications, and from hard infrastructure to data and algorithms. Furthermore, the paper situates the EU in the global technology playing field and considers vital steps to boost the bloc's digital competitiveness. Ultimately, such steps should increase the bloc's economic security—that is, the ability the EU has to make decisions and assert itself in the digital domain.[4]

The paper concludes by presenting actionable steps for the EU and its Member States on themes such as diversifying supply chains and advancing the development of European alternatives to critical dependencies. **A crucial recommendation is to strategically focus funding on areas where the EU already competes—and especially in areas where the EU can control vital chokepoints of industries, sectors or the development of particular technologies, resulting in strategic indispensability. That indispensability implies co-dependency, reducing the risk of external coercion.**

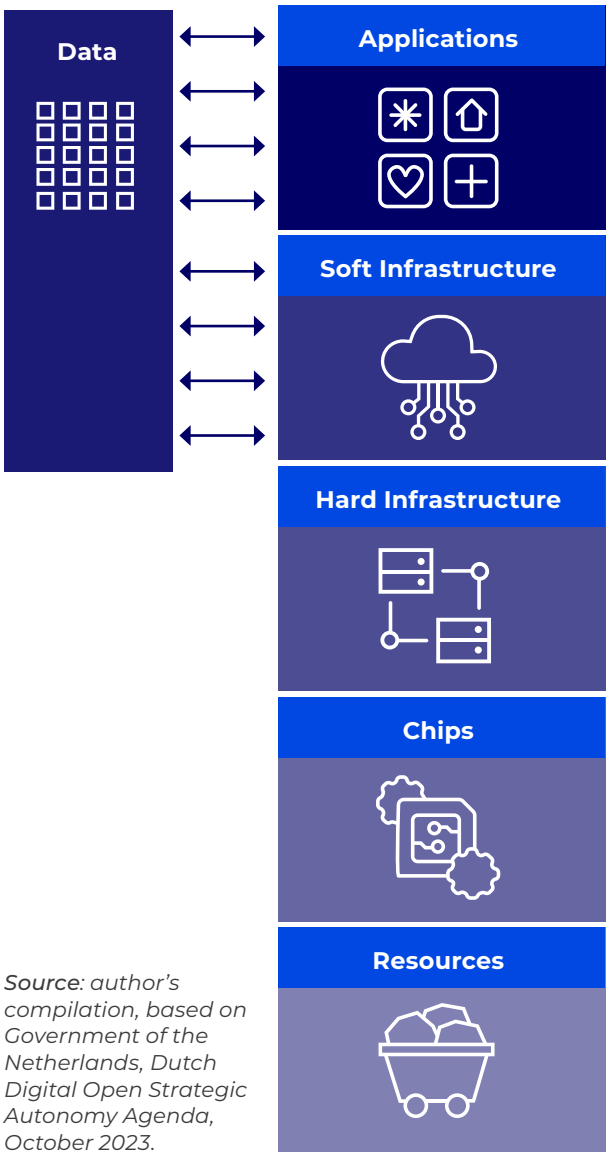
BUILDING BLOCKS OF DIGITAL TECHNOLOGY

02

02. BUILDING BLOCKS OF DIGITAL TECHNOLOGY

Digital technologies are constituted by several building blocks, also known as technology layers. The following five building blocks are critical to the upkeep of digital systems: resources, chips, hard infrastructure, soft infrastructure, data and applications (*see Figure 1*).

Figure 1: Digital Technologies Building Blocks.



Source: author's compilation, based on Government of the Netherlands, Dutch Digital Open Strategic Autonomy Agenda, October 2023.

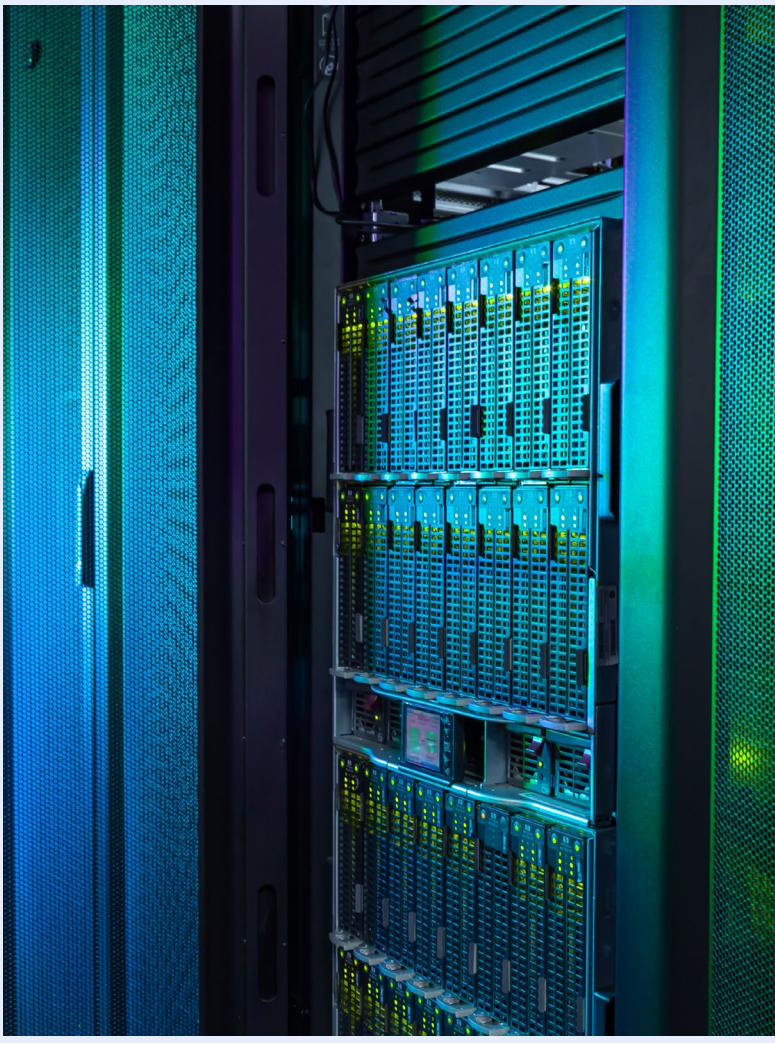
Resources herein refer to critical raw materials which are required to produce and enable the rest of technology layers, such as the silicon metal needed to manufacture computer chips. Mining and refining such materials are limited to locations that possess the resources and necessary capabilities. China dominates the CRMs supply chain: at present, few countries can rival the Chinese capacity regarding mining, refining and processing. For instance, the country is responsible for refining about 90% of rare earth elements (a subset of CRMs).[5] Resources are important for other digital building blocks, such as hard infrastructure, which has high running costs due to energy and water usage on top of the critical raw material needed for their manufacture. In this field, the EU is lagging. However, it is attempting to reduce current vulnerabilities, for instance through supply chain diversification, a topic addressed later in this paper.

The next digital building block is constituted by **chips**. Chips are electronic circuits that perform the operations behind—and at the core of—digital technologies. Chips are found in all digital products—from computers to cars and from mobile phones to modern kitchen stoves. Their growing ubiquitousness and importance, as well as the specificities of their development and supply chain, make them a particularly important and geopolitical technology piece. For this reason, the EU adopted the European Chips Act in 2023, with €80 billion mobilized in chips investments so far, to be followed up by a Chips Act 2.0 later this year.[67]

Chips are the basic unit that supports the **hard infrastructure** layer. Hard infrastructure mainly consists of connectivity systems and data centers. Connectivity is facilitated by data cables, radio masts, and all other equipment needed to build land, mobile and satellite networks that enable digital systems to communicate with each other. They are the foundation of the internet and GPS for navigation, for instance. Data centers are the physical locations where data or information is stored and processed. Many data centers in the EU are leased to or owned by US-based companies, presenting a challenge for European companies to emerge. To overcome this, the EU is now investing in AI-specific 'AI factories', for instance.[8] This paper also discusses ongoing debates around data sovereignty—the idea that sensitive data should be stored in Europe and by EU-based companies.

The next layer is **soft infrastructure**. Soft infrastructure denominates all non-physical infrastructure and services that allow organizations to quickly deploy and scale digital services. In this domain, cloud computing has fundamentally changed the way organizations develop their products and services. Cloud computing essentially means using many computers elsewhere (in a data center) to store data and run applications. This represents a paradigm shift in information technologies, which evolved since the 2010s. Traditionally, organizations used to host and manage data on local, smaller-scale data centers. With the advent of cloud computing, these services are outsourced and managed by third parties. That way, an organization avoids the capital expenses required to acquire such infrastructure and needs less in-house knowledge of computers. Cloud services are to the developer of an AI application what toll roads are to a car driver: the driver pays a small amount of money that is a fraction of the cost of building a road, such that they can simply operate their car without needing to construct a highway. This layer is dominated by US-based companies with very few European competitors, a topic of growing concern and debate about, among others, security risks.[9]

Cloud services are the foundation of the final two layers: **data and applications**. Data possessed by a company or organization can be used by algorithms, which tell the computer what operations to perform. Next to the rapid developments in chips and infrastructure over the past two decades, the ever-growing amount of data that digitalized societies generate every second is a key enabler of the current AI revolution. Simply put, algorithms implement (business) ideas that are presented or sold to users in the form of an application. For instance, that can be an AI solution like an AI chatbot, where the data has been rearranged into a meaningful text or other output format. US-based companies dominate the applications layer in the European market, from social media to e-commerce and AI applications, with notable exceptions in niches such as the strong Dutch agriculture technology sector.[10]



To illustrate how the various digital building blocks discussed above interact with each other and work in practice, *Box 1* presents the example of an AI chatbot application. Chatbots are increasingly employed on the websites of companies and governments to assist with stakeholder contact. They touch upon all issues related to an outsourced tech stack that this paper discusses below: (digital) dependencies on resources and infrastructure, the EU's digital economic deficit, and challenges regarding values.

Box 1: Description of how the various digital building blocks interact with each other in the case of an AI chatbot application.

APPLICATION LAYER

A citizen asks the AI chatbot of their government's tax administration 'How much will I pay in taxes this year?'. The AI chatbot asks follow-up questions and answers the user's question. AI chatbots present users with a simple and intuitive way to automatically answering their questions. Like chatting with a friend or family member, the user can ask their questions using their preferred natural language. OpenAI's ChatGPT, Microsoft's Copilot or Google's Gemini are well-known examples of AI chatbots.

DATA LAYER

The AI chatbot has access to the tax authority's databases, making it possible to retrieve the citizen's data and answer their questions. The tax authority's databases have all the required data—from citizens and businesses—that allow the AI chatbot to perform the necessary operations and provide the answers.

SOFT INFRASTRUCTURE LAYER

The tax authorities need soft infrastructure to develop and maintain the AI chatbot. This can be either in-house, or through a cloud software provider: Amazon, Microsoft and Google currently dominate almost 70% of the European market. Few companies have the ability to create an AI chatbot from scratch, as it requires an immense investment upfront. That is why cloud services are popular: they make applications development easier and more efficient. At the same time, dependencies on American hyperscalers raise concerns regarding data privacy and digital sovereignty.

HARD INFRASTRUCTURE LAYER

When a user poses a question to the AI chatbot, the answer will ultimately be generated in a data centre that hosts and runs the application. Data centres can easily adjust to the demand, scaling up operations and temporarily using more computers to process information in peak times—for instance, when tax statements are due and many citizens use the AI chatbot to ask questions at the same time.

Connectivity, in this case, is required to connect a user's computer or smartphone to the data centre that runs the AI chatbot.

CHIPS LAYER

Computer chips are the electronic circuits that perform the actual operations of our AI chatbot. Specialized AI chips are efficient at training and running AI algorithms that allow the computer to answer the user in natural human language.

RESOURCES LAYER

Critical Raw Materials such as silicon metal are required as a basic material to produce computer chips. Complex machines are also needed in their manufacturing, both to make the chips and test them. The related knowledge and supply chains are spread out worldwide. Additionally, vast amounts of energy are needed to keep the data centres running and water to cool the computers, which would overheat otherwise.

LIMITATIONS AND RISKS AND OF AN OUTSOURCED TECH STACK

03

03. LIMITATIONS AND RISKS AND OF AN OUTSOURCED TECH STACK

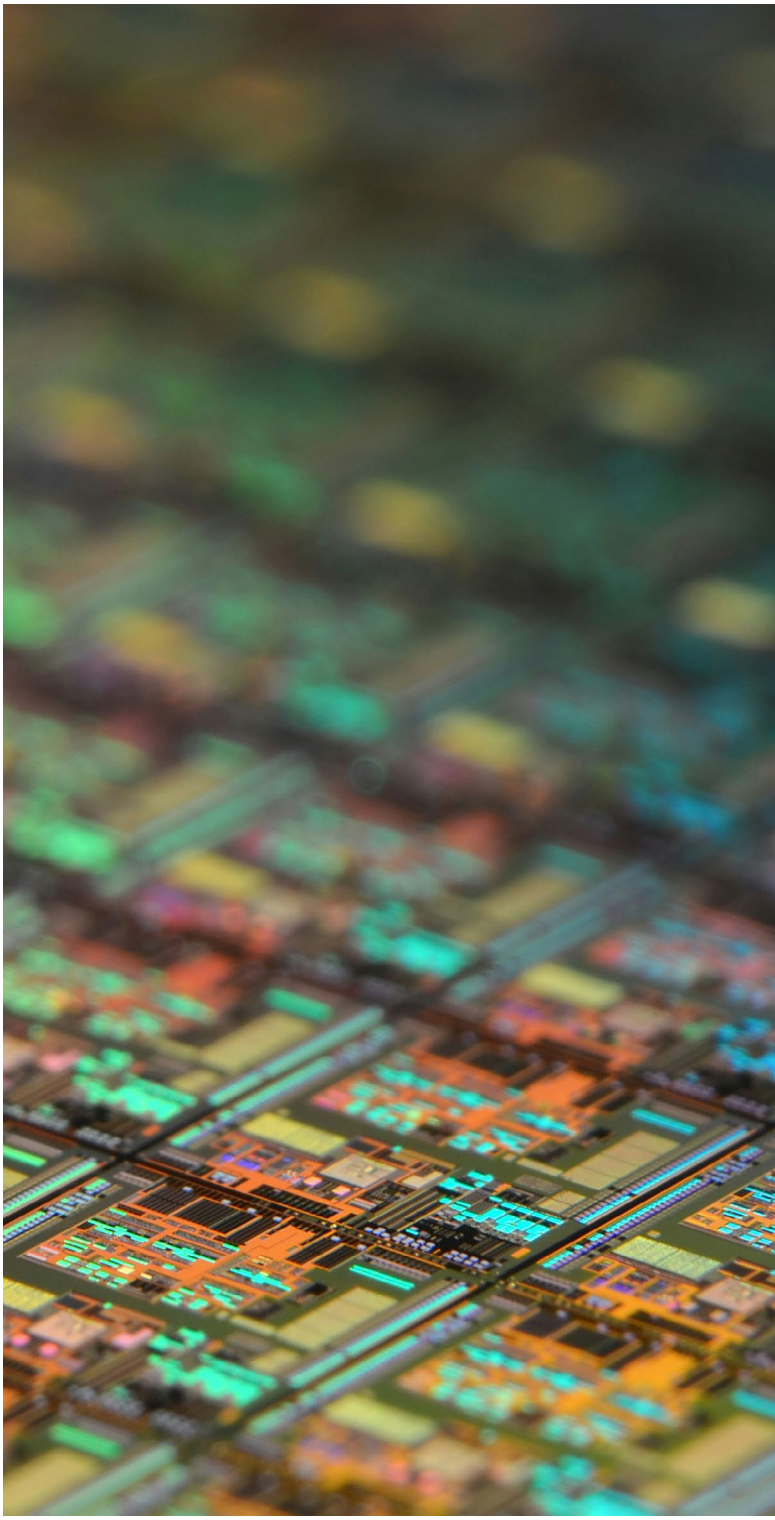
The **digital revolution** has turned computers, software, and related products into core elements of an increasingly digital economy. With different types of government and value sets increasingly colliding, such assets have become a centerpiece of the geopolitical balance of power.

The main challenges of the EU's technology stack are threefold:

- A lack of competitiveness—and hence, ownership of chokepoints—in the hardware and software layers;
- An ever-growing digital trade deficit—mostly with the US;
- And normative challenges resulting from the growing power of Big Tech companies and the fact that technologies are designed elsewhere.

Hardware and software dependencies result from that overreliance on imports, limiting supply chain resilience and risking continuity of services. From an economic viewpoint, the EU has a digital trade deficit that limits its competitiveness. Finally, differences in values such as privacy, data safety and access to reliable information mean that imported technology services contribute to a digital landscape that challenges the EU's normative approach to technology.

With different types of government and value sets increasingly colliding, such assets have become a centerpiece of the geopolitical balance of power.



3.1 HARDWARE AND SOFTWARE DEPENDENCIES AMIDST HYBRID WARFARE

The Covid pandemic exposed dependencies on third countries for crucial products, such as face masks or ventilators, which can be detrimental to the EU's interests and economy. Similarly, when it comes to products such as advanced chips or critical raw materials, such supply chain dependencies are a major geopolitical vulnerability of the EU. Advanced chips, for instance, are exported exclusively by TSMC (from Taiwan) and Samsung (from South Korea), with 92% of the worldwide production concentrated at the former manufacturer.[11]

Beyond these physical goods, the EU also overly relies on US-based cloud providers such as Microsoft Azure, for most of its data storage and software needs. Specifically, the three biggest American Cloud Service Providers (CSPs)—Amazon Web Services (AWS), Microsoft Azure and Google Cloud—jointly hold about 'nearly 70% of the global Infrastructure-as-a-Service market', while European Cloud Service Providers (CSPs) lack behind at a mere 10%.[12] The EU's overreliance on these essential products and resources could be weaponized in—at least—two main ways: they could be withheld to trigger a direct crisis on the would-be receiving end, or the provider could use the threat of cutting off access as leverage during a conflict.

Additionally, the EU's heavy reliance on cloud services on countries from outside the bloc comes with significant (cyber) security risks. Data that is stored outside the EU could be copied, altered, leaked or deleted without the consent of the owner. Imagine, for instance, citizens' student debts being annulled or altered without leaving a trace of their original values. All such records would have to be ignored, leading to big losses for the government. Such attacks could be launched on most government services, causing widespread chaos. The digital transition coincides with increased hostilities worldwide, including acts of 'hybrid warfare'. Hybrid attacks operate at the interface between war and peace by remaining sufficiently small and potentially committed in disguise as accidents or acts by non-state actors.[13] They aim to disturb or hinder societies without provoking a full-scale traditional armed response. Using foreign cloud services increases societies' exposure to such hybrid attacks. As Henry Farrell and Abraham Newman put it, 'the same networks that knit the world together also allow powerful states to spy, sabotage, and sanction'. **Interdependence is not inherently risky—it becomes dangerous when one side is available to use it as a tool of coercion.**

The EU's overreliance on these essential products and resources could be weaponized in—at least—two main ways: they could be withheld to trigger a direct crisis on the would-be receiving end, or the provider could use the threat of cutting off access as leverage during a conflict.

3.2 DIGITAL TRADE DEFICIT

Besides geopolitical and security risks, the overuse of imports and overreliance on foreign digital services contributes to the widening of an already significant gap in capabilities.

To begin with, the EU has a digital trade deficit—mostly with the US. The term digital deficit is commonly used in Japan to define the balance between imports and exports of digital services.[14] **Over 80% of digital infrastructure and technologies in Europe are currently imported.[15] A key example of this is the cloud market, with most EU cloud consumers buying their services from US-based CSPs.[16]** Such a deficit is undesirable, as it reflects the economic impact of dependencies in areas like cloud and AI services. Investments in European alternatives to American CSPs would allow them to scale and bring missed revenue to the EU's single (digital) market. That would free up money for research and development by European players rather than reinforcing their US-based competitors, allowing them to close the offerings and knowledge gaps over time.

Secondly, Big Tech companies choke local alternatives where physical resources are concerned. Their economic power and ability to influence decision-making allows them to build and expand data centers at a much higher pace than their European counterparts, which have a lot of difficulties expanding their own facilities.[17] The (negative) environmental impact that data centers take on electricity networks and water usage is exacerbated by the fact that, most often, the economic benefits of data centers usage does not stay in Europe.

Lastly, vendors lock-in ties new customers to the dominant Big Tech companies. For example, by pre-installing certain services that are difficult or impossible to uninstall from a device; by reducing interoperability between systems by implementing proprietary standards; or by using unfair pricing mechanisms to lock out competitors.[18] These practices often jeopardize European competitors and present challenges that the Digital Markets Act aims to address.

3.3 NORMATIVE CHALLENGES: VALUE MISALIGNMENT WITH US AND CHINESE BIG TECH COMPANIES

A few large companies, mostly concentrated in Silicon Valley in the US, dominate the digital services landscape. Their dominant position spans from social media platforms and cloud services to chip design and reflect into a myriad of normative challenges to the EU in several building blocks of the technology stack.

3.3.1 PRIVACY CONCERNS

One of the biggest contention points between the EU's approach to technology and digitalization and that of great powers like the US and China relates to privacy protection. Privacy concerns stem from two main factors. Firstly, Big Tech business models rely on collecting and retrieving as much data from their users as possible, to process and resell it for purposes that are not beneficial to the user. Personalized and targeted advertising services, for instance, are among their biggest sources of revenue.[19] Secondly, there is a small, yet nonzero chance that the data stored by these companies may be requested or accessed by US intelligence agencies, under national security grounds and extraterritorial laws such as the CLOUD Act, Foreign Intelligence Surveillance Act (FISA) and the Defense Production Act.[20] Although the probability of data misuse under these (American) regulations is low, data can easily be weaponized. Europe has historical reasons to be particularly sensitive to this topic: the registration of religion in state records is an example of seemingly benign data collection ending up a catastrophe, helping the Nazis find the dwellings of Jewish people during World War II.[21]

One of the biggest contention points between the EU's approach to technology and digitalization and that of great powers like the US and China relates to privacy protection.

The dominance of very few social media platforms means that their leaders effectively control the algorithms that determine the media consumption patterns of many EU citizens.

3.3.2 OMINOUS 'TECH BROS'

In ancient Greece, citizens of Athens would meet at the Agora for political debates. Presently, EU citizens are more likely to debate on a US-based or Chinese online social medium. Major US-based social media platforms include Instagram, X (formerly known as Twitter) and Facebook. They are run by CEOs Elon Musk and Mark Zuckerberg who, together with figures such as Amazon's executive chairman Jeff Bezos and Sundar Pichai (CEO at Alphabet, Google's parent company), have attained immense political influence.[22] The close ties between US Big Tech and the Administration were visible at the 2025 inauguration ceremony of US President Donald Trump, where the Big Tech CEOs were placed in front-row seats.[23]

These CEOs have begun to explicitly influence US and European democracies through campaign donations, publicity stunts or even direct involvement. Musk, for example, has been appointed the leader of an officious 'Department of Government Efficiency' of the US, with the (officious) mandate to eliminate government jobs and functions he and his team consider unnecessary.[24] The influence of these 'tech bros', as this group has been called,[25] also extends deeply into European democracies. On the one hand, Musk has publicly endorsed and interviewed European politicians leading up to elections, helping the political far-right gain a fresh and tech-savvy image. On the other hand, the dominance of very few social media platforms means that their leaders effectively control the algorithms that determine the media consumption patterns of many EU citizens.

TikTok is a social media platform headquartered in Singapore and San Francisco, US, but owned by the Chinese ByteDance. It is unique in its ability to compete with the various large US-based social media channels. TikTok is the subject of heavy debate: concerns over potential Chinese espionage and social engineering have led many governments and companies to ban their employees from using the application.[26] The idea that a Chinese company could control the news intake of a significant proportion of citizens worries many politicians and observers. However, there are others who have voiced that they prefer absolute freedom of speech and view a potential ban of the app as undue censorship. Notably, the new Trump administration has undone a ban on TikTok by President Joe Biden. Vice-President JD Vance delivered an ill-received speech to EU policymakers at the Paris AI Summit in February 2025, dismissing EU legislation meant to curb misinformation as a form of undemocratic censorship. Vance called the policies 'massive regulations … about taking down content and policing so-called [emphasis added] misinformation' meant to 'to prevent a grown man or woman from accessing an opinion that the government thinks [emphasis added] is misinformation.'[27] These statements explain the sudden permissive stance of the US vis-à-vis TikTok and exhibit the value gap regarding technology between the current US Administration and the EU.

3.3.3 FAKE FACTS AND ERRONEOUS EPICS REPLACING TRUE TALES

The right to and need for accurate information is undermined by social media applications and the propagation of AI bots.[28] This right is a vital basis of functioning democracies. Three factors play critical roles in this process: the spread of disinformation on social media platforms, misinformation from AI bots, and reduced income for traditional media platforms.

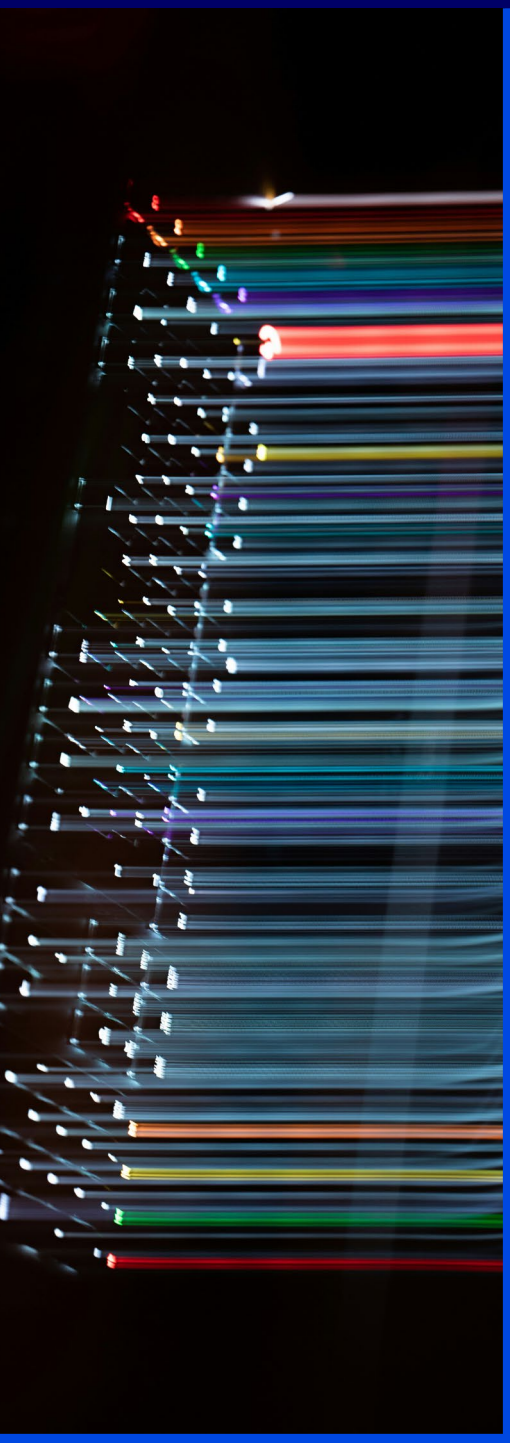
> Both the US-based social media platforms and TikTok can easily be abused by foreign actors to influence elections and spread disinformation,[29] as their algorithms amplify misinformation to increase engagement.[30]

Russia, for instance, employs workers with the specific goal of spreading Russian propaganda and disinformation and boosting far-right parties in foreign democratic elections.[31] EU legislation targets these issues, namely via the Digital Services Act enacted in 2024, but is increasingly challenged by American Big Tech, well represented in VP Vance's speech in Paris. American social media platforms no longer feel as compelled to comply with EU regulation as before, as they are backed by their governments to ignore EU laws. The EU, for its part, will face a huge challenge in implementing the twins Digital Services Act and Digital Markets Act: in addition to the political attrition highlighted above, the question of whether the required instruments and resources are available—both at the European and Member States level—to enforce compliance remains unanswered.

On top of social media, AI bots also negatively affect the access to correct information in two ways. First, AI models that are at the core of AI chatbots are ultimately very advanced prediction tools. However, a crucial limitation is that this advanced guesswork makes AI-powered tools prone to generate inaccurate answers by making up facts or sources. This limitation is recognized by developers and may be overcome even in the near future but still occurs in most AI chatbots. Secondly, AI models are inherently biased. This bias depends on the choice of data that has been selected to train and configure the AI model, which can be programmed to avoid giving certain types of answers. As AI usage increases, the power of setting biases—and thereby an agenda or a particular worldview—grows along. That power is concentrated in the hands of a small number of (mainly US-based) AI companies, demonstrating a vulnerability for democracies everywhere.

Meanwhile the income of traditional media houses, like newspapers and broadcasters, has declined. The shift of readers to social media, where they tend to only read headlines or brief summaries, fails to generate revenue for the original news sources. AI chatbots and AI-generated content are another culprit. Underlying AI models are often trained on texts from traditional outlets without proper compensation. The decline of trusted news sources seriously threatens democracies, as they play a crucial role in verifying information and providing essential platforms for trustworthy public debate.

> American social media platforms no longer feel as compelled to comply with EU regulation as before, as they are backed by their government to ignore EU laws.



ACTIONABLE NEXT STEPS

04

04. ACTIONABLE NEXT STEPS

The vulnerabilities stemming from the EU's largely outsourced tech stack call for action. The EU Commission subscribes to this view, as evidenced by the various pieces of legislation and funding strategies put forward in the EU Competitiveness Compass. Notable areas of rulemaking efforts include the Digital Services Act and Digital Market Act on online safety, and digital markets and competition, and the AI Act to promote human-centered AI. Examples of initiatives to stimulate digitalization in the EU bloc are the EU's Digital Decade program and, more recently, the InvestAI initiative.[32] Given the current technology gap and digital deficit of the EU, there is scope for additional policy plans and actionable next steps.

The following section focuses on potential ways for the EU to cooperate with third countries, against the backdrop of the current geopolitical context. Next, the policy paper engages with several building blocks and technology layers, namely soft infrastructure, chips and supply chain resilience, all with a view to increasing the EU's (digital) economic security

4.1. KEY PLAYERS AND THEIR POLICIES

The EU motivation to strive for digital economic security is becoming more widely understood and accepted.

> The growing US-China technology and tariffs dispute initiated by President Trump in his first Presidency, the Covid pandemic and the Russian war of aggression in Ukraine were important triggers over the past five years for Europe to realize that dependency comes at a cost.

Recognizing that the digital transition has made most sectors and industries heavily dependent on chips, soft infrastructure and software, which are to a great extent imported from elsewhere, has been another key step. Importantly, this includes sectors such as defense and missions such as the green transition. Even in sectors where computers and chips have not entered the production process directly, globalization and international shipping have become the standard in most supply chains and heavily rely on advanced information systems. As such, digital economic security is inherently about much more than just the technology market. Striving for digital economic security means that the EU aims to foster competitiveness, resilience and security across the technology stack.

To achieve greater autonomy, the EU must understand and engage various key players discussed next. The 'protect/promote/partner' framework that underpins the EU Economic Security Strategy allows for concrete policy paths.[33] The goal is enhanced engagement and collaboration with partners that share the EU's interest in maintaining a rule-based world order and secure cooperation with those that only share limited interests and values with the EU.

THE UNITED STATES:
BRING SENSITIVE DATA HOME

The EU and its Member States have long collaborated with the US on technology, and ever-growing dependencies have not been highly contested until recent years. The most notable EU dependencies on the US on tech include cloud and AI applications, as well as e-commerce and other big platforms, which have far-reaching implications for digital governance and legislation. EU laws increasingly clash with the US approach to technology, with the second Trump Administration emphasizing values such as absolute freedom of speech over the right to correct information, or the dangers of misinformation. With the US now casting doubt over the Transatlantic partnership in the military realm, too, dependencies on US-based cloud service providers have become a significant risk to critical systems and citizens' privacy. As such, **the EU's mission is to help public and private sector organizations dealing with sensitive data or fulfilling vital societal functions move to EU-based competitors.**

CHINA:
COLLABORATE WHERE POSSIBLE, DE-RISK WHERE NECESSARY

The EU's relationship—and that of particular Member States—with China is highly complex and two-faced. China is an important trading partner, which supplies the EU with a wide range of products at a highly competitive price point. At the same time, China's values on technology do not align with those of the EU. Namely, China is often considered a key challenger of the liberal world order that the EU stands for, and its approach on technology has been casted as 'digital authoritarianism'.[34] Furthermore, overreliance on China is potentially dangerous: China could limit exports of Critical Raw Materials as a geopolitical tool, leaving the EU with no viable alternatives in the short term. The EU's approach of 'de-risking' from China focuses on maintaining mutually beneficial open trade channels where possible, while diversifying critical supply chains as needed. **The Global Gateway initiative offers ample opportunities for cooperation with the private sector in providing economically viable alternatives to China-dominated supply chains.**

INDO-PACIFIC:
COOPERATE ON OVERLAPPING VALUES AND INTERESTS

As many question the current US' commitment to defending the rule-based international order, one avenue for EU's diplomacy and foreign policy is to double down its cooperation with countries like Japan and India. Regarding digital governance, both Tokyo and New Delhi share a commitment to protecting the present (yet shifting) world-order and promoting democracy, openness and fairness. India's leadership on Digital Public Infrastructure, through its "India Stack" of digital services and its "Aadhaar" digital identities, have allowed the country to develop a flourishing tech scene and promote similar initiatives in multilateral relations. Japan's high-tech economy goes hand-in-hand with its commitment to developing a solid industry in the production of CRMs. Furthermore, both countries share with the EU their complex relationships with China. On the one hand, they rely on China for crucial trade that helps their economies thrive. On the other hand, they are wary of overdependence on China, which has not shunned coercion through export controls in the past and has an increasingly assertive military stance in the Indo-Pacific. These shared interests make India and Japan into potentially vital allies if the EU is to diversify its supply chains beyond China and towards more similar partners. Moreover, collaboration with countries that share the EU's values and vision of a liberal world stage helps grow and promote such ideas globally. Therefore, the EU-India Trade and Technology Council meeting late February, reinvigorating the forum after a nearly two-year hiatus, and initiatives such as the EU-Japan Strategic Partnership are most welcome. To promote trilateral cooperation, a meeting would help explore how the ample existing bilateral cooperation platforms are best expanded.

ASSOCIATION OF SOUTHEAST ASIAN NATIONS (ASEAN):
ENHANCING CONNECTIVITY AND STANDARDS

In a bid to promote good data governance, improve digital connectivity and enhance the digital economy and financial technologies, the EU would benefit from greater collaboration with ASEAN. **Although options for deeper cooperation with ASEAN are scarce due to the variety of ASEAN members and their diverse attitudes vis-à-vis the EU, China, and other countries, a baseline model built on the minimum set of rules and standards all parties can agree on could be instantiated.** That would already simplify trade and potentially deepen ties. In December 2020, the EU and ASEAN adopted a Joint Ministerial Statement on Connectivity, demonstrating the parties' willingness to cooperate.[35] The two blocs strengthened their commitment early 2024, when new sustainable connectivity projects were announced under the Brussels' Global Gateway scheme.[36] Warmer ties can help foster easier trade with ASEAN members, and the (Digital) Global Gateway agenda can assist the EU in diversifying its supply chains.

AFRICA:
LEVERAGING GLOBAL GATEWAY TO BUILD PARTNERSHIPS ON CRITICAL RAW MATERIALS

The EU's overreliance on China for its CRMs has prompted it to look to resource-rich countries in Africa to diversify its supply chains. Particularly, the EU has signed Memoranda of Understanding with the Democratic Republic of Congo (DRC) and Zambia to develop cooperation on supplying CRMs.[37] For these potential partnerships to materialize, it is key that the EU mobilizes its private sector, aided by Global Gateway initiatives. However, **any investments must also benefit the local economy, to ensure that the EU's presence is a sustainable and better alternative to China's Belt and Road Initiative propositions.** Furthermore, the EU might benefit from aligning its efforts in Africa with those of countries such as Japan, India and the US, increasing mutual trust and cooperation with those partners.

LATIN AMERICA
COLLABORATION ON SUSTAINABLE CRITICAL RAW MATERIALS SOURCING

The 2023 Association Agreement with Chile marked a first step in the EU's ambitions to diversify its CRM supply chains to benefit from Latin America's vast deposits of, primarily, lithium and copper. Notably, the parties agreed that the cooperation should include a strong focus on labor rights and high environmental standards.[38] The EU has since continued to invest in CRM supply chains in Latin America, in alignment with its Global Gateway initiative that seeks to entice the private sector into strategic investments.[39] This renewed interest in Latin America contributes to a mutually beneficial deepening of the EU's ties with the continent; Bolivia, for instance, has the world's largest lithium deposits but has no means to develop its reserves locally.[40] Similar to the EU's efforts in Africa, **the EU could benefit from aligning its efforts with partners that share an interest in supply chain diversification.**

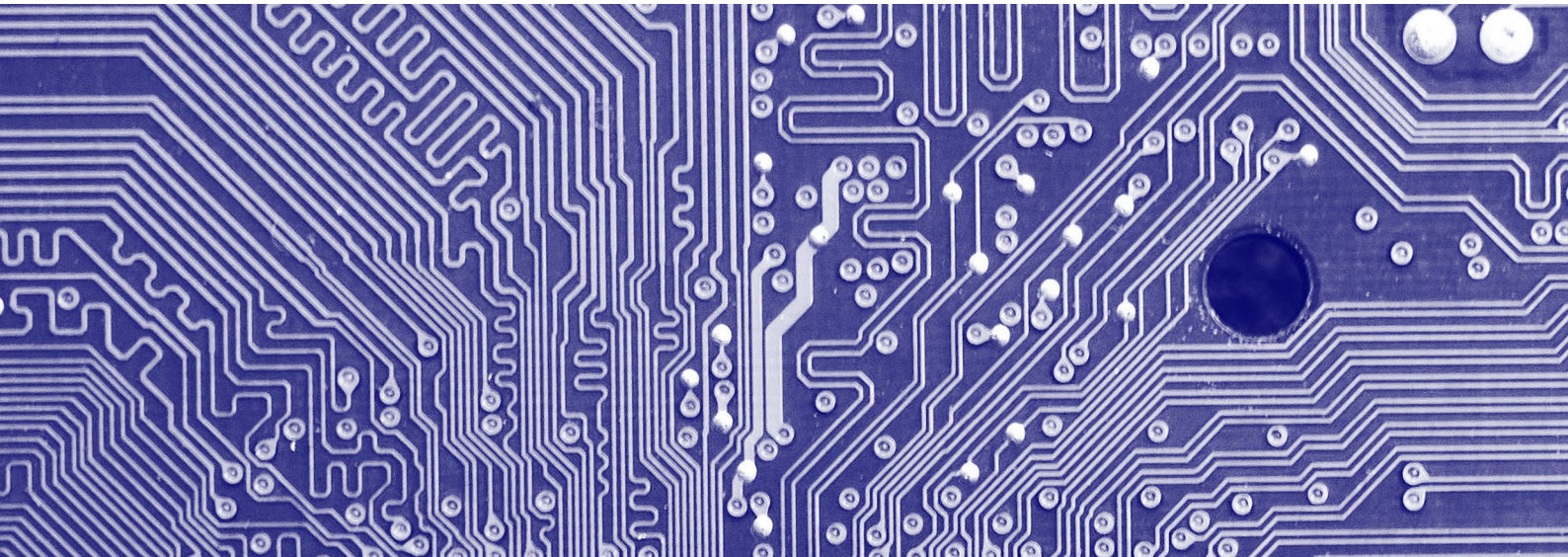
4.2 DEVELOPING EU-BASED SOFT INFRASTRUCTURE

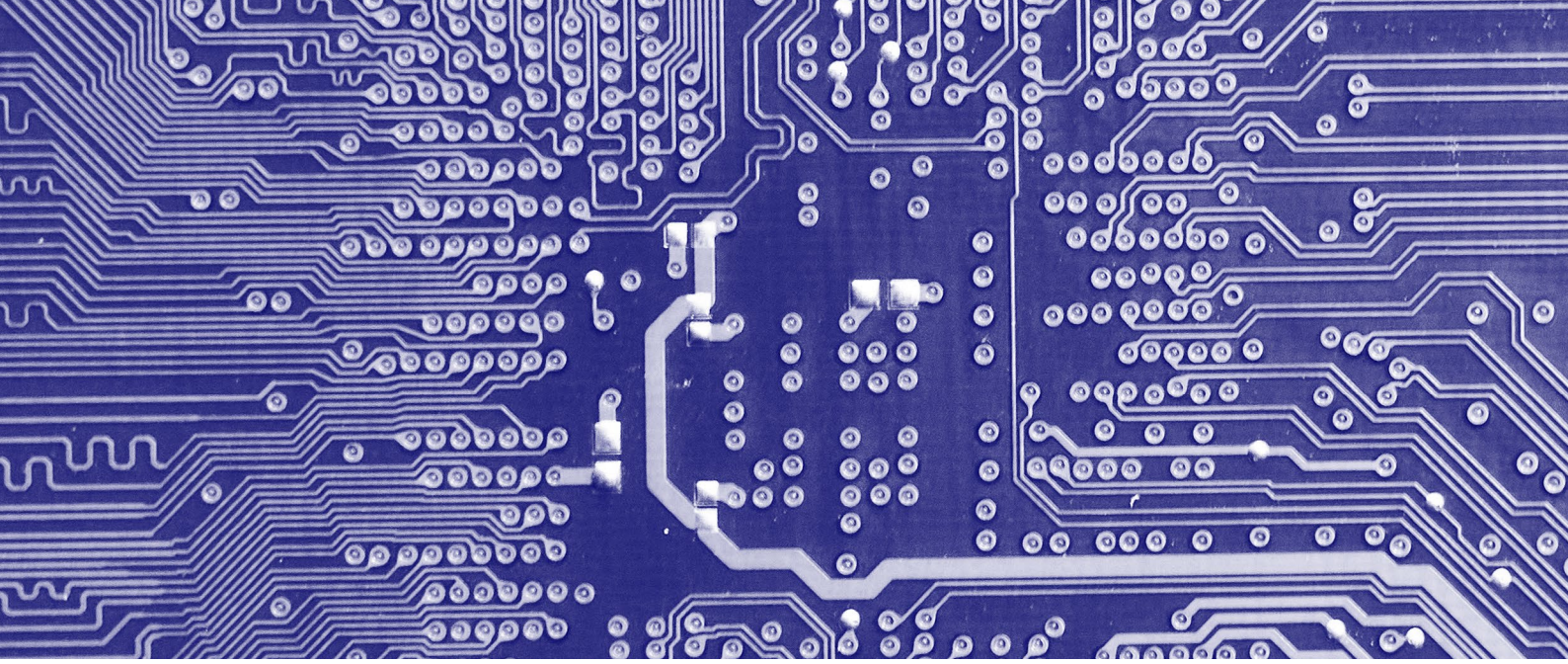
US-based Cloud and AI services dominate the EU market, based on different values and giving rise to risks of overreliance. A promising development is the recent emergence of Schwarz Group's (parent of German retailer LIDL) 'STACKIT', a European cloud platform and the latest big hope in the European CSPs landscape. Other European players of relevance are OVHcloud, Aruba Cloud, Ionos, Leaseweb, Scaleway or Hetzner. Astute industrial strategy and policy are essential to help such 'European champions' grow into the much-needed market leaders they might become.

For instance, the EU could update its public procurement processes to prefer European products where possible. Besides, the EU could help European companies access the electricity grid, space and water for data centers. It could also time-limit concessions for non-European data centers, based on the Norwegian model: when Norway began to use hydropower, it gave companies short-term concessions that could be renewed or discontinued based on present needs. Similarly, its oil fields were discovered by private sector companies that were allowed to profit from their discoveries for some time before Norway decided it would continue on its own. Comparable strategies could work for data centers, as it is not necessarily in the EU's interest to continue to allow US-owned data centers and IT infrastructure to be foreign-owned indefinitely, forgoing crucial resources for local competitors. In the light of such foreign-owned data centers, it is also important to factor in externalized costs. **The pressure that data centers put on electricity grids and water usage, for instance, must not be carried by European countries when the profit made crosses into the US.** The European Commission is currently developing the AI and Cloud Development Act, expected to be published by the first quarter of 2026, which will focus on and may become a vital instrument to address these challenges.

While initiatives like GAIA-X were launched to foster European data sovereignty and develop (federated) infrastructure, the project has faced significant challenges in terms of strategic clarity, adoption and commercial value. Despite its ambition, GAIA-X has yet to demonstrate broad traction among key stakeholders or deliver clear value, especially in addressing Europe's structural scale disadvantage in the digital domain. **The EU could prioritize creating rules to support existing commercial solutions rather than building alternatives from the ground up.**

The EU could update its public procurement processes to prefer European products where possible.





4.3 MAINTAINING INDISPENSABILITY AND STRATEGICALLY FOCUSING FUNDING

To limit its exposure to coercion, the EU can increase and maintain its indispensability in digital supply chains. ASML is the most obvious example of a vital European tech company, particularly in the advanced chips supply chain. The company currently dominates the lithography equipment field with no notable challengers. Therefore, the EU is not just dependent in the advanced chips realm but has an ace of its own. As such, the chances of barriers to trade or, at worst, the full withholding of certain produce, are significantly lower than they would be in a relationship with a one-way dependency.

National governments can play a critical role in investing in their local industries, providing the conditions such companies need to thrive. That includes housing, education and other competitive regional advantages.[41] The EU's industrial policy and collective investment schemes help too, and would benefit from closer alignment with the Multiannual Financial Framework (MFF). Instruments embedded within the MFF—such as Digital Europe, Horizon Europe, and cohesion funds—should be more strategically focused on building digital sovereignty in areas like cloud, AI infrastructure and chips.

A stronger mobilization of private capital is also needed. The InvestEU programme, which aims to unlock over €372 billion in public and private investment, offers a powerful tool to de-risk strategic projects and crowd in private investment. Better integration of MFF-funded instruments with InvestEU guarantees can ensure a coherent investment pipeline across Member States.

> Maintaining indispensability in key areas is essential as it is a more feasible short-term aim than catching up with competitors in all fields. A similar rationale of strategically focusing funds could help in other areas too.

EU Member States do not need to excel in all areas, but rather should focus on staying or getting ahead in a few main areas each. Such specialization could lead to increased cooperation and services trade across Member States, leading to more efficiency. However, this requires making difficult decisions on which (promising) sectors should be promoted, for example through research funds. Those national decisions can benefit from coordination on the EU level. The completion of the EU Single Market would certainly help a shift in the right direction, making it easier for companies to do business across borders.

4.4 SUPPLY CHAIN RESILIENCE THROUGH DIVERSIFICATION

Critical raw materials that are vital for the production of chips are mostly imported from China. The EU has recently begun to invest in improving relations with alternative suppliers, such as Ukraine, Canada, and various countries in Central Asia and Africa. These efforts are bolstered by the Critical Raw Materials Act and the Global Gateway project, as exemplified by investments in Kazakhstan's CRM sector.[42] As the geopolitical climate continues to harshen, engaging with partners with similar interests is increasingly important to guarantee the EU keeps having access to edge technologies. This urgence is also felt by the recently renewed EU Commission, whose first diplomatic visit was to India in an effort to work with that country on collectively diversifying supply chains. In India, EU Commission President Ursela von der Leyen said that 'by investing together in this tech [AI] and by building strong supply chains, we can create a real advantage for ourselves in today's competitive global economy'.[43] An essential aspect of diversifying supply chains is collaboration between the EU and private sector partners. Ultimately, businesses control supply chains and thus need to be on board with and implement any changes. EU Member States can help the EU Commission identify opportunities for such shared public/private initiatives, as they best know their economies and companies.

The Global Gateway's digital pillar can serve as an entry point for establishing mutually beneficial cooperation, as a basis for engagement on supply chain diversification. For such projects to deliver an initial quick win, EU Member States can inventory the particular strengths of partner countries' tech sectors. Then, smaller projects with a direct effect can be implemented, fitting well to the local context by listening to partner countries needs and wishes. The focus does not need to be on large, hard infrastructure projects, but could rather be on smaller, sector-specific applications where many Member States have something to offer in certain domains.[44]

An essential aspect of diversifying supply chains is collaboration between the EU and private sector partners. Ultimately, businesses control supply chains and thus need to be on board with and implement any changes.

05. CONCLUSIONS

The EU faces a range of geopolitical challenges related to its digital and technological agendas, notably surrounding economic security, data confidentiality and value rifts with key technology providers. Many such challenges stem from undue dependencies on third countries that spur worries over the availability and suitability of critical building blocks of the European technology stack. Recent geopolitical developments, particularly worrying trends in the US since President Trump's return to the Oval Office, have only exacerbated and highlighted such issues. For example, Vice-President Vance's speech at the Paris AI summit demonstrated that the US' values no longer align with those of the EU regarding democracy and the right to correct information.

Simultaneously, the very developments that cause legitimate concern have indeed shocked the EU and the bloc is starting to move into action. For example, the EU Commission's visit to India in late February can be seen as an attempt to increase collaboration with alternative and increasingly important partners. In that regard, initiatives such as the EU's Global Gateway can help, too. In collaboration with the private sector and Member States, the EU Commission can work with existing and new partners to diversify its supply chains and reduce dependencies. For instance, a minilateral tech engagement with Japan and India is an opportunity that deserves to be explored. Others, such as United Kingdom and Canada, can also be involved. At the same time, efforts to keep leading EU companies like ASML ahead of the international competition, maintaining indispensability in the supply chain of (AI) chips—a fundamental building block of the (AI) technology stack—, must feature at the core of EU's industrial policy.

Diversification of raw materials supply chains and hard infrastructure is best pursued hand in hand with investments in EU-based soft infrastructure. The EU would benefit from updating its public procurement laws to reflect the new geopolitical realities, prioritizing local cloud and services providers. This is most critical for organizations dealing with sensitive data, such as governments or companies in sectors like health or education. Prioritizing products and services from European players would channel investments into EU-based cloud providers, potentially improving their long-term competitiveness.

Civil society has also been active in advocating for enhanced digital economic security and plays a vital role in defending a technology stack based on EU interests such as democratic values, privacy, and the twin green and digital transitions. Research projects like the EuroStack make the case for EU tech sovereignty.

> After the first mandate of European Commission President Ursula von der Leyen focused on creating the rules of a fair digital game in Europe, the next five years will be make-or-break for the EU's ability to bolster its digital economic security—and, ultimately, its sovereignty—in the long run.

ENDNOTES

1 European Commission, Europe's Digital Decade: Digitally empowered Europe by 2030, March 2021.

2 Mario Draghi, The Draghi report on EU competitiveness, September 2024.

3 Eurostack, The EuroStack report, February 2025.

4 Maaike Okano-Heijmans, Alexandre Gomes and Daniel Kono, Strengthening digital economic security: Promote, Shape, Regulate and Protect, please!, October 2023.

5 International Energy Agency, Energy Technology Perspectives 2023, January 2023.

6 Euractiv, Virkkunen confirms a Chips Act 2.0 and outlines AI action plan, March 2025.

7 Reflecting on a crucial challenge in the years ahead, a case study on AI chips will be published in May

8 European Commission, AI Factories | Shaping Europe's digital future, March 2025.

9 WIRED, Trump's Aggression Sours Europe on US Cloud Giants, March 2025.

10 Alexandre Gomes and Maaike Okano-Heijmans, Dutch niches for Global Gateway Policy Brief in the digital domain: An initial enquiry, October 2023.

11 European Parliament, The EU chips act: securing Europe's supply of semiconductors, 2023.

12 Bertelsmann Stiftung, EuroStack—A European Alternative for Digital Sovereignty (p. 66), February 2025.

13 NATO Review, Hybrid Warfare—New Threats, Complexity, and 'Trust' as the Antidote, 30 November 2021.

14 The Japan Times, Japan's trade deficit for digital services rose to record ¥6.6 trillion in 2024, 11 February 2025.

15 Bertelsmann Stiftung, EuroStack—A European Alternative for Digital Sovereignty (p. 8), February 2025.

16 Bertelsmann Stiftung, EuroStack—A European Alternative for Digital Sovereignty (p. 66), February 2025.

17 Time, Big Tech Is Coming to Small-Town America, But There's a Catch, 4 August 2021; Data Centre Dynamics, Updated: Dutch province of Flevoland enforces temporary data center moratorium, 15 June 2021.

18 Euronews, Apple hit with €62 million EU class action for unfair charges on music, 18 September 2024.

19 Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, 2019.

20 Alexandre Gomes and Maaike Okano-Heijmans, Too late to act? Europe's quest for cloud sovereignty, March 2024.

21 De Correspondent, In de Tweede Wereldoorlog hadden we wél wat te verbergen (in Dutch), 8 May 2014.

22 The New York Times, 'Effectively Unaccountable': Inside the Trump-Musk Relationship, 5 February 2025.

23 Associated Press, Trump, a populist president, is flanked by tech billionaires at his inauguration, 21 January 2025

24 BBC, 'People seem dumbstruck'—Inside Musk's race to upend government, 6 February 2025.

25 Financial Times, Have we hit peak tech bro?, 3 February 2025.

26 The German Marshall Fund, TikTok Tactics: 2024 US Candidates Dance Around Security Risks, 30 October 2024.

27 The American Presidency Project, Remarks by the Vice President at the Artificial Intelligence Action Summit in Paris, France, February 11, 2025.

28 AWS, What is a Bot?

29 BBC, Misinformation v disinformation: What's the difference?

30 New York Times, How Social Media Amplifies Misinformation More Than Information, 13 October 2022.

31 European Union External Action, 2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence, January 2024.

32 European Commission, EU launches InvestAI initiative to mobilise €200 billion of investment in artificial intelligence, 11 February 2025.

33 European Commission, An EU approach to enhance economic security, 20 June 2023.

34 Tony Roberts and Marjoke Oosterom, Digital authoritarianism: a systematic literature review, 24 November 2024.

35 Clingendael Institute, Growing stronger together: Towards an EU–ASEAN digital partnership?, February 2022.

36 European Commission, Global Gateway: EU and ASEAN strengthen their partnership on sustainable connectivity, 2 February 2024.

37 Africa Policy Research Institute, Navigating Critical Mineral Supply Chains: the EU's Partnerships with the DRC and Zambia, March 2024.

38 European Council on Foreign Relations, Critical material: The EU's and Chile's new relationship in the multipolar world, 14 December 2023.

39 European External Action Service, Global Gateway: New EU-IDB Initiative to Boost Sustainable Critical Raw Materials Practices in Latin America and the Caribbean, November 2024.

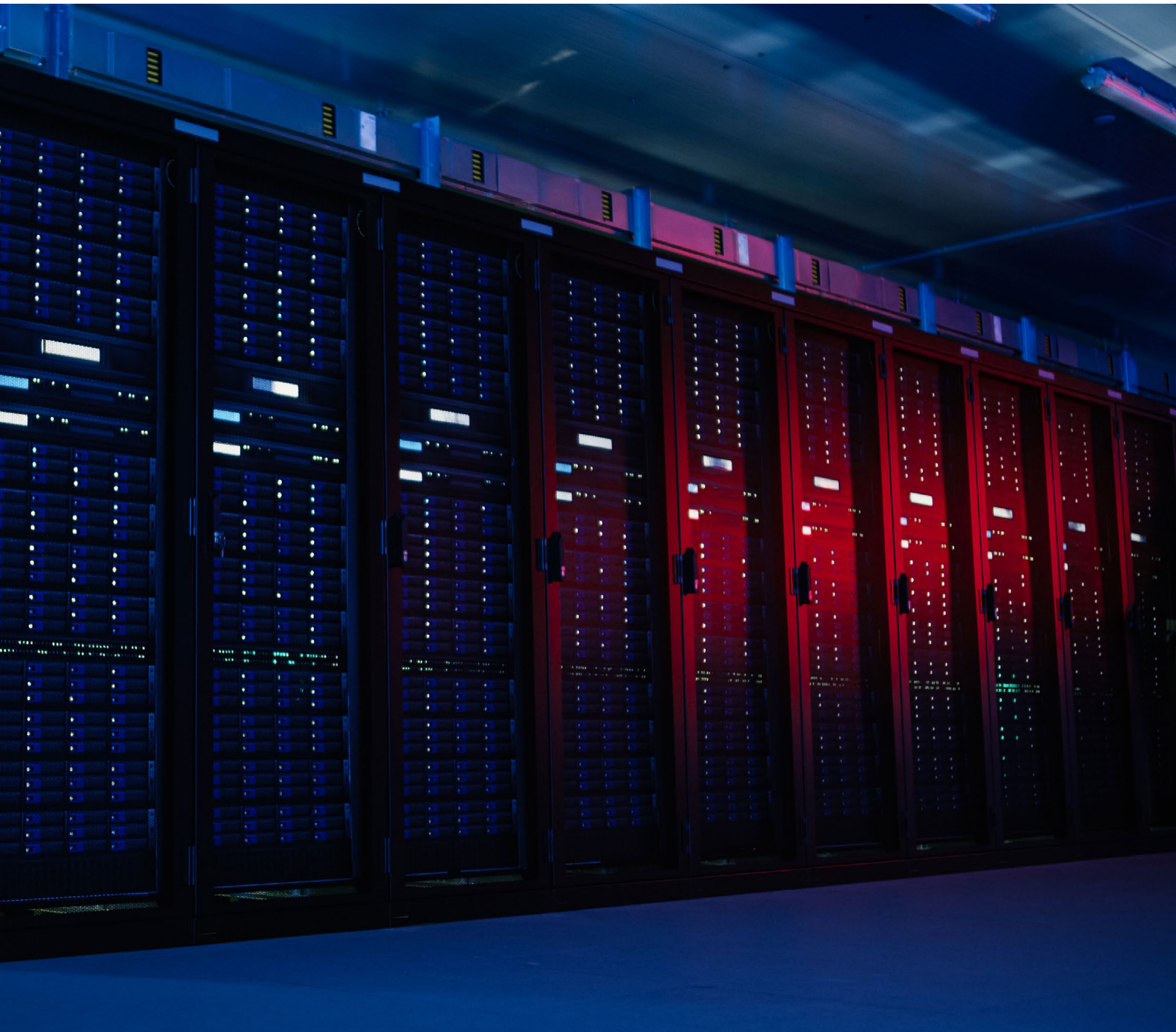
40 European Parliamentary Research Committee, EU–Latin America: Enhancing cooperation on critical raw materials, December 2024.

41 For example, see the Dutch 'Project Beethoven': Dutch Government, The Netherlands to invest €2.5 billion to strengthen business climate for chip industry in Brainport Eindhoven, April 2024.

42 Delegation of the European Union to the Republic of Kazakhstan, EU and Kazakhstan advance Global Gateway Strategy with key agreements, 13 March 2025.

43 European Commission, Speech by President von der Leyen: 'The Consequential Partnership: Reimagining and realigning EU and India ties for today's world', 28 February 2025.

44 Alexandre Gomes and Maaike Okano-Heijmans, Harnessing the potential of Digital Global Gateway: Towards sector-specific applications, February 2025.



AUTHORS:
Alexandre Ferreira Gomes, Maaike Okano-Heijmans and Jelle van den Wijngaard (*Clingendael Institute*)

RECOMMENDED CITATION:
Ferreira Gomes, A., Okano-Heijmans, M., & van den Wijngaard, J., *Beyond Lego: The Need for EU-Based Building Blocks of Technology*, IE CGC, April 2025.

Design: epoqstudio.com

Images: Unsplash, Shutterstock.

cgc.ie.edu