cerre Centre on Regulation in Europe

DIGITAL INDUSTRIAL POLICY FOR EUROPE

REPORT

December 2022

Paul Timmers

As provided for in CERRE's bylaws and procedural rules from its "Transparency & Independence Policy", all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The project, within the framework of which this report has been prepared, received the support and/or input of the following CERRE member organisations: Intel, Qualcomm, and Vodafone. However, they bear no responsibility for the contents of this report. The views expressed in this CERRE report are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond either to those of CERRE, or of any sponsor or of members of CERRE.

info@cerre.eu – www.cerre.eu

TABLE OF CONTENTS

GLOSSARY....4
ABOUT CERRE....5
ABOUT THE AUTHOR....6
EXECUTIVE SUMMARY....7
1. INTRODUCTION....9
2. PERSPECTIVES ON INDUSTRIAL POLICY....11
3. ANALYSIS FRAMEWORK....17
4. APPLYING THE THREE PERSPECTIVES TO SELECTED CASES....22
4.1. Semiconductors....22
4.1.1 General....22
4.1.2 Analysis of situation....23
4.1.3 Analysis of EU semiconductor policy....26
4.2. Cloud and Platforms....31
4.2.1 General....31
4.2.2 Analysis of situation....33
4.2.3 Analysing EU cloud policy....34
4.3. Digital Identity....40
4.3.1 General....40
4.3.2 Analysis of situation....40
4.3.3 Analysis of EU digital identity policy....42
5. INSIGHTS FROM THE SELECTED CASES....44
5.1. Methodological....44
5.2. Institutional Capability and Capacity....44
5.3. Policy Completeness....45
5.4. Policy Consistency....45
5.5. Digital Industrial Policy as Integrated Policy....46
5.6. Risks and Pitfalls....46
6. POLICY RECOMMENDATIONS....49
6.1. Industrial Strategy and Geopolitics....49

6.2. Digital Industrial Policy Development 49
6.2.1 Completeness 49
6.2.2 Consistency 49
6.2.3 Impact 49
6.3. Priorities for digital industrial policy 50
6.4. Policy Responding to the Nature of 'Digital' 50
6.5. Specific digital industrial policies 51
6.5.1 Semiconductors 51
6.5.2 Cloud 51
6.5.3 Digital identity 51
6.6. Institutional Capacity and Capability 51
7. CONCLUSIONS AND NEXT STEPS TOWARDS AN EU DIGITAL INDUSTRIAL POLICY WORKPLAN 53
ANNEX I: ADDITIONAL THEORETICAL BACKGROUND 54
Industrial policy interventions 54
International relations (IR) 55
National competitiveness, industrial ecosystem 58
ANNEX II: CASES IN DETAIL 60
Case: Semiconductor Policy and the EU Chips Act 60
Case: Trusted Cloud and EU Cloud 62
Case: Digital Identity and EU Digital Wallet 63
REFERENCES 65

GLOSSARY

CEF	Connecting Europe Facility (EU funding programme)
DA	Data Act (EU legislation)
DGA	Data Governance Act (EU legislation)
DIP	Digital Industrial Policy
DMA	Digital Markets Act (EU legislation)
DSA	Digital Services Act
eIDAS	Electronic Identification And trust service (EU legislation)
FDI	Foreign Direct Investment
GDPR	General Data Protection Regulation (EU legislation)
HSM	Hardware Security Modules
IP	Intellectual Property
IPCEI	Important Project of Common European Interest
IR	International Relations
R&D	Research and Development
R&I	Research & Innovation
RRF	Resilience and Recovery Fund ((EU funding programme)
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
TTC	Trade and Technology Council (EU-US)

ABOUT CERRE

Providing top quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) promotes robust and consistent regulation in Europe's network and digital industries. CERRE's members are regulatory authorities and operators in those industries as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach;
- the widely acknowledged academic credentials and policy experience of its team and associated staff members;
- its scientific independence and impartiality;
- the direct relevance and timeliness of its contributions to the policy and regulatory development process applicable to network industries and the markets for their services.

CERRE's activities include contributions to the development of norms, standards and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological and social environment. CERRE's work also aims at clarifying the respective roles of market operators, governments and regulatory authorities, as well as at strengthening the expertise of the latter, since in many Member States, regulators are part of a relatively recent profession.

ABOUT THE AUTHOR

Prof Dr **Paul Timmers** is a research associate at the University of Oxford, Oxford Internet Institute, professor at European University Cyprus, visiting professor at KU Leuven and the University of Rijeka, senior advisor EPC Brussels, President of the Supervisory Board Estonian eGovernance Academy and CEO of iivii. Previously, he was Director at the European Commission/DG CONNECT where has held responsibility for legislation and funding programmes for cybersecurity, eID, digital privacy, digital health, smart cities, and e-government. At the European Commission, he was also a cabinet member of European Commissioner Liikanen. He worked as manager of a software department in a large ICT company and co-founded an ICT start-up. He holds a physics PhD from Radboud University (Nijmegen, NL), MBA from Warwick University (UK), EU fellowship at UNC Chapel Hill (US), and a cybersecurity qualification from Harvard. His main interests are digital policy, geopolitics, and Europe. He frequently publishes and speaks on the interplay of digital developments with sovereignty, cybersecurity, industrial policy, and sectoral policies such as digital health and is regularly advising governments and think tanks.

EXECUTIVE SUMMARY

Digital industrial policy is the deliberate attempt by government to orientate industrial development in the digital domain towards specific paths. This study addresses digital industrial policy at EU level.

Digital industrial policy is 'hot' in Europe. 'Digital' has become pervasive across economy, society and democracy and is the key determinant of future jobs and competitiveness in the EU. Europe and the world are profoundly, perhaps even existentially, challenged by climate change, war, and cyber threats. Their consequences include mass displacement, social unrest, and economic shocks. 'Digital' is both the major opportunity to deal with these challenges and part of the problems. Geopolitical tensions have risen dangerously. The relationship of the US and the EU with China disrupts global business. Strategic autonomy and sovereignty concerns have become *Chefsache*. The open global market economy and borderless digital infrastructures are no longer the marker on the horizon.

These challenges call for a break from the past in our approach to industrial policy. Firstly, industrial policy is no longer a taboo. Secondly, geopolitics is now a determinant of industrial policy. Thirdly, digital industrial policy must be relevant to the transformative, disruptive, and global nature of digital technologies. Therefore, digital industrial policy can be the trailblazer of a new perspective on industrial policy.

Above all, the EU must get a stronger position in the digital industrial world in order to safeguard internal and external legitimacy, that is, the sovereignty of its Member States and the EU itself.

Industrial policy deals with industrial ecosystems to build and strengthen national and EU competitiveness and jobs, which are public goods. Industrial policy is also concerned with individual firms to ensure that the interests of companies and public interests align. This is traditional industrial policy. The novel approach is to address upfront geopolitics as a determinant of industrial policy *and* to relate the three levels of policy action: industrial policy in relation to geopolitics, industrial policy to shape the industrial ecosystem, and industrial policy to address firm-level concerns.

The analysis in this report builds on three major cases for digital industrial policy: semiconductors, cloud, and digital identity. The report provides general and case-specific recommendations. The main general recommendations are:

1. Apply the three-level methodology – geopolitical, industrial ecosystem, firms – prioritising digital industrial policy that brings in key EU user industries and the core of government.
2. Extend institutional capability and capacity for EU-level and national digital industrial policy development, notably to coherently integrate internal and external policy interventions.
3. Pro-actively monitor and act on risks and pitfalls for digital industrial policy starting with actions on critical dependencies (chokepoints).

The main case-specific recommendations are:

- Semiconductors: complement the EU Chips Act with a fully geopolitical approach, that addresses geopolitical developments, including the risk of conflict such as subsidy races. This can build on

international co-operation with 'like-minded' partners, notably with the USA such as in the TTC, and include a rolling impact assessment on investments and funding.

- Cloud: develop industrial policy analysis for edge cloud; consolidate cloud policy actions into an EU cloud industrial policy and/or edge cloud industrial policy, including the international impact
- Digital identity: urgently come forward with a digital identity EU industrial policy, coherently integrating existing actions and complementing or extending these, where needed, to safeguard EU sovereignty.

The analysis approach of this study results in rich insights. There is, however, much work ahead for the EU to develop a comprehensive, coherent and complete digital industrial policy. This report provides both the way to do so and the priorities to consider.

1. INTRODUCTION

Industrial policy is "a deliberate attempt by the government […] to orientate industrial development towards specific paths" (Bianchi & Labory, 2020)[1]. In the modern view, it addresses the industrial ecosystem as a whole.

Industrial policy can act on investment, R&D, standardisation, private-public collaboration, commercial behaviour, etc. (Aggarwal & Reddie, 2018) define market-creating, market-facilitating, market-modifying, market-proscribing, and market-substituting actions. A generalisation of these to the industrial ecosystem is used in this report[2].

In traditional industrial policy such actions have to correct market failures. The types of industrial policy are either 1) where policy is not specific to industry but affects the industrial environment, such as social policy and general educational policies or 2) where policy is specific to an industry, which can be split into either 2a) policy that is not for a specific industry such as general R&D programs, or 2b) policy for a specific industry such as public procurement of specific technologies or specific R&D funding (Figure 1).

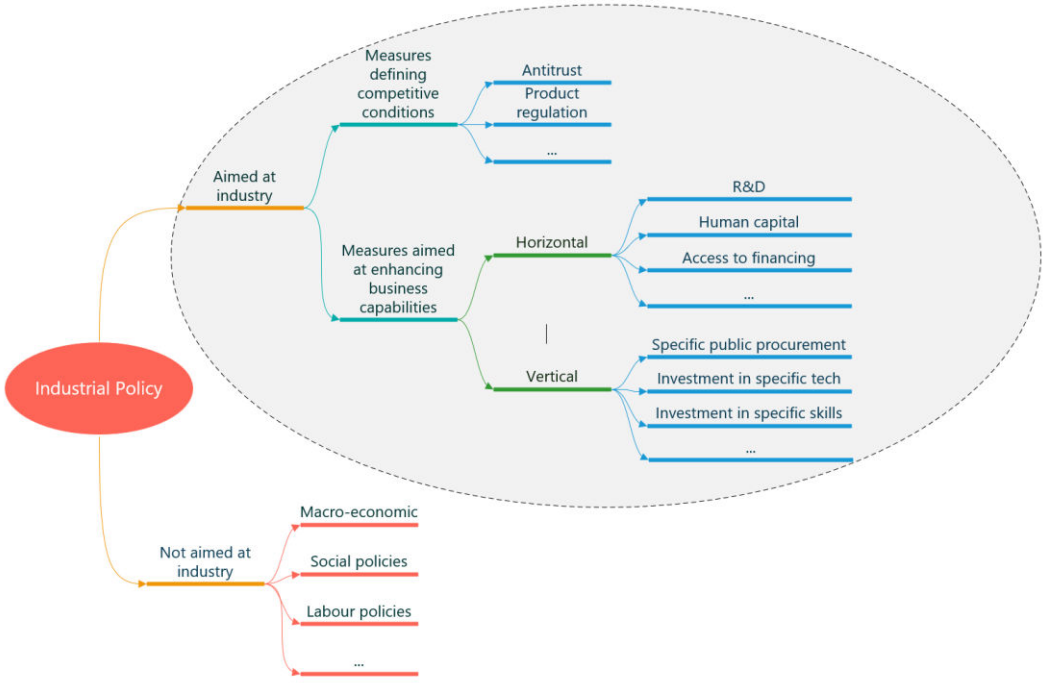


Figure 1: Types of industrial policy, after (Bianchi & Labory, 2020). Digital industrial policy is in the shaded area.

Industrial policy used to be mostly about strengthening competitiveness and improving the functioning of markets. Recently other objectives increasingly influence industrial policy thinking. The first objective is strategic autonomy, i.e., the control, capabilities and capacities (3C) necessary to

[1] A range of industrial policy definitions is in Aiginger & Rodrik (2020).
[2] See annex I.

safeguard and strengthen sovereignty[3]. (Waltz in Art & Jervis, 2016, p. 56) states "that a state is sovereign means that it decides for itself how it will cope with its internal and external problems"[4]. The second objective is resilience, which has become particularly prominent due to supply-side shocks in energy, semiconductors, and rare earths, and the demand/supply-side shocks of pandemic and war. Resilience is a necessary but not sufficient condition for sovereignty. Finally, very much on the rise is the objective of 'saving the planet, or 'greening' i.e., improving sustainability[5].

Modern industrial policy will therefore likely be multi-purpose. But the purposes of today are different from the past and need more urgently than ever to be addressed. Sovereignty and war are existential for the EU. The planet is existential for all of us[6]. When one of the purposes is sovereignty, industrial policy is a contribution to strategic autonomy, which consists of the capabilities (what we know), capacities (how much we can do), and control in the industrial ecosystem necessary to safeguard sovereignty.

Our focus here is on digital industrial policy (DIP). 'Digital' merits special attention as the digital world has become huge[7], very geopolitical, and confronts us with unprecedented speed of development, scale, and systemic effects. These effects are even more amplified when several digital innovations are pursued in synchrony. Ever more digital policies are being tabled in the EU, almost always with industrial relevance. This raises the question, what the overall strategy in and approach to digital industrial policy for the EU should be. We will answer that question in this report.

[3] Strategic autonomy is here defined as Control, Capabilities and Capacities (3C) to decide and act on essential aspects of the economy, society and democracy (Timmers, 2022b). Strategic autonomy in a specific area, such as digital, materials, health, or finance, is labelled correspondingly, i.e., digital strategic autonomy, materials strategic autonomy, etc. Somewhat confusingly, the term digital sovereignty is often used as a synonym for digital strategic autonomy.

[4] There are many more definitions and descriptions of sovereignty, see e.g., Biersteker (2012), Klabbers (2021, p. 75),Bickerton et al. (2022), and Glasze et al. (2022). Waltz's definition is rather absolute, whereas, in reality, there are degrees of sovereignty, which corresponds to strategic autonomy not being absolute either (Timmers, 2021).

[5] For an analysis of the history of industrial policies see E. Cohen (2022).

[6] E. Cohen (2022, p. 154) eloquently argues that geopolitics and the energy transition give new legitimacy to industrial policy.

[7] The World Economic Forum (2019) states that 70% of new value created in the economy over the next decade will be based on digitally enabled platform business models.

2. PERSPECTIVES ON INDUSTRIAL POLICY

Perspectives on industrial policy are changing. Failures of past industrial policy have led to much soul-searching[8]. Doubts about economic ideology, in particular about the 'Washington Consensus'[9], also played a role in challenging or even outright rejection of established wisdom on industrial policy.

There is, however, nowadays a renewed appreciation for industrial policy and in particular of manufacturing and innovation (Aiginger & Rodrik, 2020), mission-oriented industrial policy (Mazzucato & Kattel, 2020), and technology dynamics (Coyle & Muhtar, 2021). The French and German governments' Manifesto of 2019 stresses the importance of manufacturing and calls for massive investment in innovation. There is a rebalancing between competition and industrial policy to address market failures. The Manifesto calls for regulatory adaptation pointing to new approaches to competition rules given distortive support by third countries[10].

Thinking is also evolving on the balance between openness to global markets and protection of EU markets, where the European Commission suggests that multilateralism, open markets, and (open) strategic autonomy can be joined up[11]. The 'open' in open strategic autonomy means continued support for an open global economy and multilateralism[12]. For the EU in particular there is also a strong awareness and even some pride that EU internal market can give international leverage of EU regulation. (Bradford, 2020) calls this the 'Brussels Effect'. While it has not been explicitly formulated as such, EU industrial policy too may get international leverage by such a Brussels effect. However, (Renda, 2022) argues that next to market size also first-comer lead in market regulation plays a role in such international influence. Given the speed of (digital) industrial policy development in China, a 'Beijing Effect' is to be taken seriously.

In this report, digital industrial *policy* in general and in specific cases is analysed. Where policy directs the action and thinking of others, strategy directs our own thinking and action. This report is substantially also about digital industrial *strategy*[13]. Key elements of the digital industrial strategy developed here are to put geopolitics on equal footing with competitiveness and business performance as drivers of industrial strategy (leading to a 'geopolitical industrial policy') and to respond to the radically different quality of the digital world.

Digital industrial policy deals with the digital industry, which is a very broad industry. The analysis in this report of semiconductors, cloud and digital identity shows that each digital area requires specific and well-tuned industrial policy actions. Nevertheless, we will provide a general method to develop

[8] Such reflection also happens in the EU (for an example in this context, see the semiconductor case and in particular the staff working document related to the EU Chips Act, (European Commission, 2022)). There are also successful examples of industrial policy in the EU such as in telecommunications (GSM), fabless design (ARM), aerospace industry (Airbus), space industry (Ariadne), and car safety (Infineon, NXP).

[9] The Washington Consensus is the economic view which emphasizes open liberal free-market macro-economic policies, trade liberalization, deregulation, privatization, and property rights protection. It is related to but not to be confused with neoliberalism.

[10] (French and German Governments, 2019).

[11] (European Commission, 2021b, p. 3).

[12] The European Commission's DG Trade says "making the best possible use of the opportunities of our openness and global engagement, while assertively defending our interests, both internally and externally" (European Commission, 2021a).

[13] In fact, the geopolitical thinking in this report largely also holds for industrial strategy in other domains than digital.

such policy. There are many more parts of the digital industry for which it is pertinent to develop industrial policy. Figure 2 gives one way – a technology stack – to divide up the digital industry, ranging from quantum technologies to artificial intelligence (AI) to 'Industry 4.0'. A complementary way is to take a theme that cuts across several layers. An example is cybersecurity, which cuts from secure chips at the lowest level in the stack all the way up to protection of large-scale digital infrastructures. Yet another way is to start from key industries that are users of digital technologies. This report recommends a prioritisation of areas of digital industrial policy.

DIP is conditioned by many factors and forces. Limitations in factor conditions of financial, human, territorial, material and energy resources make choices necessary. This report provides in the three cases examples of such choices.

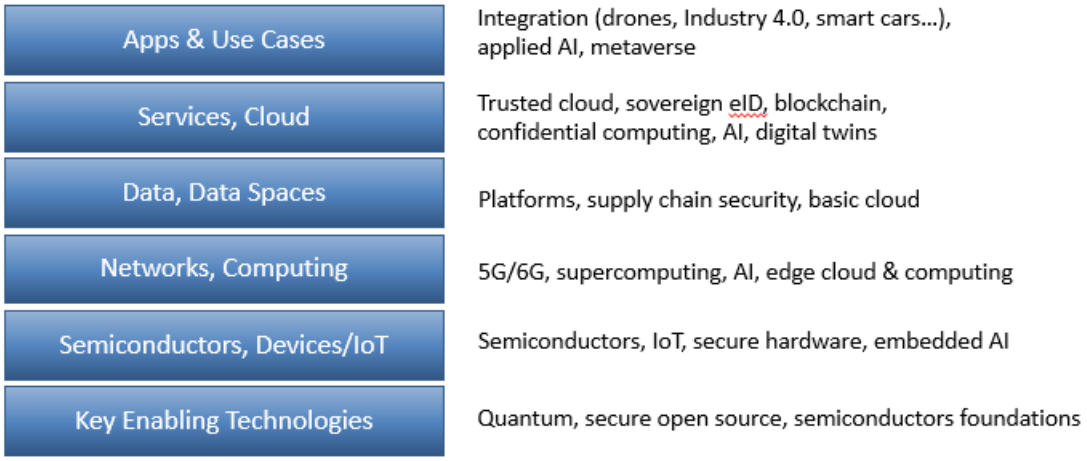


Figure 2: Technology stack view of digital industry

DIP is influenced by the macro-level forces of geopolitics, global threats, and digital technology developments. In geopolitics, we consider relations between states (what academics call International Relations or IR). Geopolitics is characterised by increasing tensions between states, bipolarisation USA-China, and even war at scale, notably the war in Ukraine. At geopolitical level we also consider the role of the big global digital players such as the large digital platforms and cloud companies. Both state and non-state actors impact and even unsettle the international system of states, contributing to what (Kello, 2017) calls a sovereignty gap. Global threats include sustainability of the planet, pandemics, and cybercrime.

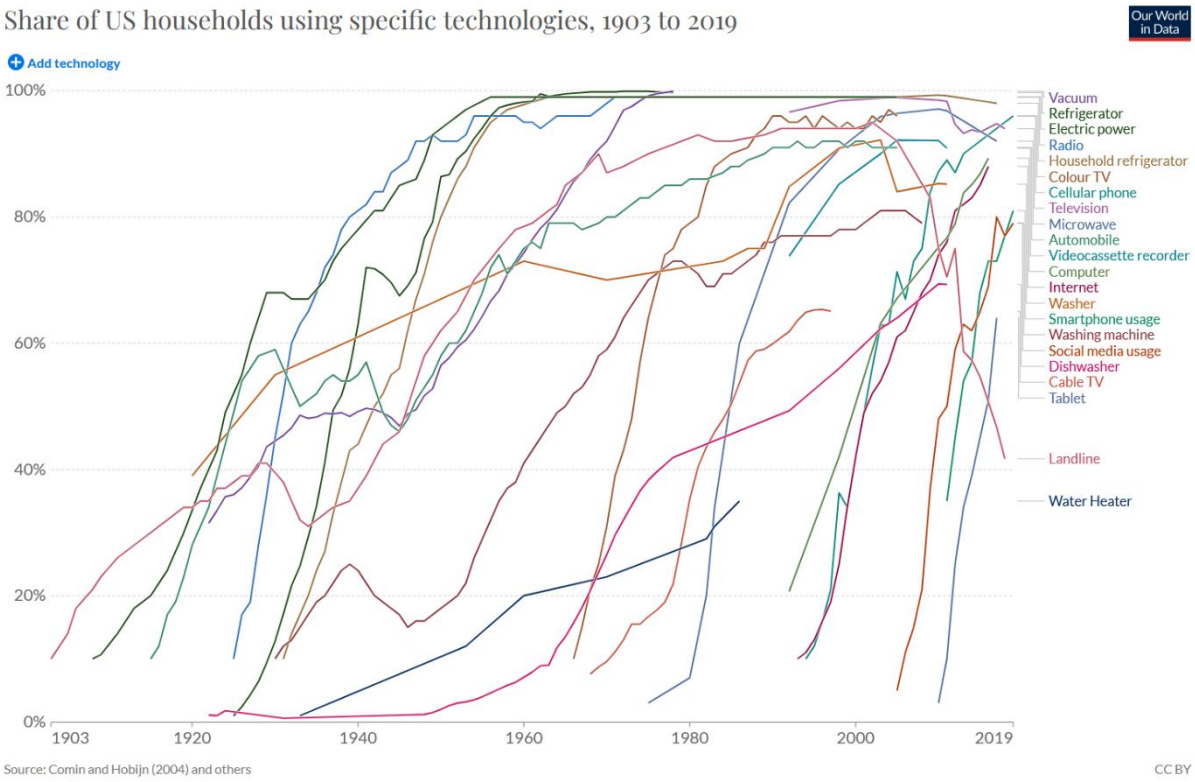
From a geopolitical view the appreciation of 'digital' is changing. Once the internet was seen as being without borders, an utopian cyberspace in which there was no place for governments and sovereignty, as (Barlow, 1996) said. Today, it is rather the opposite. A recent report is blunt: "[…the…] utopian vision became just that: a vision, not the reality. Instead, over time the internet became less free, more fragmented, and less secure. Authoritarian regimes have managed to limit its use by those who

might weaken their hold and have learned how to use it to further repress would-be or actual opponents"[14].

How digital technology develops is a major factor that DIP must take into account. First of all, it must assess the relevance of new technologies that continue arising (such as the metaverse). Secondly, it must respond to the unique speed, scale, systemic, and increasingly synchrony (4S) that generally characterises digital technology developments.

- **Speed**: there is no expectation to generally slow down digital technology development and diffusion (notwithstanding that dangerous specific technology developments may have to be put under control) but DIP policy must meet speed with flexibility. As Figure 3 shows, time to reach a level of 80% of adoption of a new technology has roughly halved in the last 20 years and continues to accelerate. This means that in the next 10 years we may see at least 3 major digital innovations that change our lives. (McKinsey, 2022) identifies as main trends metaverse, Web3, applied AI, industrialised machine learning, cloud/edge computing, digital identity), 5G/6G, quantum technologies, and next-gen software development.

Figure 3: Accelerating technology adoption (Ritchie & Roser, 2019)



- **Scale**: increasingly EU Member States realise that digital industrial policy is best dealt with together, at least at EU level or even wider, internationally. Countries are too small to deal with digital technology on their own. Therefore, national digital industrial policy heavily refers to and

[14] Council on Foreign Relations, 2022.

relies on EU-level digital industrial policy. Scale makes DIP different from much traditional industrial policy. Another aspect of scale is that certain technologies (cloud, social media, AI) have strong network effects, enabling well-resourced first-mover companies to take-it-all and become dominant in their field. They operate businesses with huge turnovers and valuations, and their positive and negative impacts on economy and society have been extensively described. In the USA and China those companies are aided by strong risk-financing. In recent years, regulators and policy makers have come up with a number of countervailing/corrective measures to market dominance, notably competition cases and regulatory initiatives such as the Digital Markets Act (DMA), to correct or prevent abuse of dominance, and what (Zuboff, 2019) calls surveillance capitalism, as well as predatory take-overs, threat to state sovereignty, etc. Generally, this behaviour has led to a loss of trust in and credibility of large digital industry. DIP has therefore to be prepared for a public credibility gap if policy actions appear to support large digital industry or neglect smaller players[15]. Big claims of DIP on limited public budgets will have to be democratically defended too.

- **Systemic**: a digital technology and its related ecosystem can affect several socio-economic systems, even more so as systems get connected. One of the most recent examples is the chips supply shortage, which affects many user industries, from automotive to turbines to defence[16]. In turn, chips manufacturing is dependent on a huge number of inputs (materials, tools, subassemblies) coming from many countries. There is massive re-use of open-source software components across many industries. Malware in administrative IT can well jump over into hospital IT, as happened with the Wannacry ransomware attack in 2017[17]. The EU requires by law[18] to address systemic ICT resilience in the financial sector since loss of trust in banks can be highly infectious. 5G will interconnect a complex system of cars, road-side computing, and large-scale traffic management. How to keep such a system robust and resilient and upgradable? Small changes in one part (one company, one piece of technology) can have significant amplified effects on other parts of the related economic, social, or technological system[19]. Systemic risks have become a major concern in the use of cloud and other ICTs in the financial sector, in the disruption of supply chains due to missing materials or natural disasters or war, and in AI-amplified social platforms. DIP must address the wider context of user industries, other digital technologies, and systemic effects.

- **Synchrony**: In addition to speed, scale and systemics, the digital industry also increasingly shows signs of synchrony, meaning that some companies – especially the digital giants – are able to combine two or more emerging technologies such as AI and cloud, AI in cyber, quantum and cloud,

[15] Questions have been raised about subsidies to semiconductor giants, and the presence of cloud giants in GAIA-X.
[16] (Chakraborty, 2022).
[17] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack.
[18] (European Commission, 2020b).
[19] Supply chain analysis can give insight into such dependencies, though psychological effects, e.g., loss of trust due to disruption, may be hard to foresee (the archetypical example being a bank run).

chips and quantum, blockchain and IoT, cloudification and 5G/6G[20]. This increases industrial opportunity but also risks of monopolisation, winner-takes-it-all, and lock-in. Generally, synchrony enhances industrial, societal, and geopolitical disruption and the breaking down of silos. Combinations are AI and cyber, quantum and cloud, semiconductor chips and quantum, blockchain and IoT, chips and crypto and IoT, and cloudification of networks (5G/6G). For DIP that means two things: firstly, to link-up specific DIPs, e.g., for semiconductors and quantum technologies. Second, to be aware with a specific DIP of opportunities and threats coming from outside that specific technology (e.g., future AI giants may take control the whole value chain of digital identity / wallets).

Some of the effects of the above qualities of 'digital' are exemplified in:

- The rapid establishment of oligopolies, such as the digital platform companies;[21]
- Battles for capital and brains – with significant brain-drain from the EU to the USA22 – and for intellectual property – with patent wars, patent hoarding, state-led (cyber-)theft of IP, and capture of standardisation by control of essential patents;
- Software achieving global usage along various pathways, such as dominance of companies, international standardisation, or low-barriers to reuse through open source;
- Shifting boundaries between public and private sector, and between civil and military;
- Shifting norms and values and ethics, often driven by opaque processes;
- Resilience risks and sovereignty threats; securitisation and militarisation.

For this report, it is important to stress that European countries are strongly digitally dependent on foreign countries, namely for over 80% of digital products, services, infrastructures, and intellectual property. This dependency is notably on the USA and has been growing over the past 10 years (see Figure 4). At the same time the USA end Europe are for 75-90% of semiconductor production dependent on Asia[23]. Digital dependencies due to complex global value chains, pervasiveness of digital, and digital as a new military domain manifest themselves in chokepoints. These are being analysed in China, the USA, and the EU.

[20] Synchrony is not to be confused with the (technology-based) convergence of telecoms and information technology, a theme of the last 20-30 years.
[21] EU policy did not anticipate this. An illustration is the cloud and platforms case, see section 4.2.
[22] (Anderson, 2022).
[23] (See diagrams in Miller, 2022, pp. 164–165).

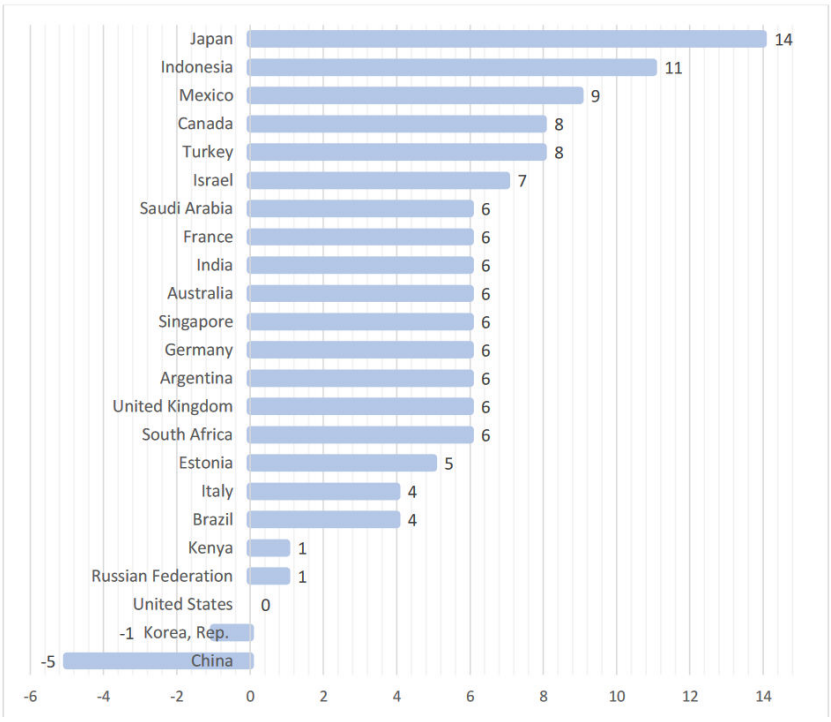


Figure 4: Digital dependency on the USA has increased except for China and S. Korea (Mayer & Liu, 2022).

3. ANALYSIS FRAMEWORK

The approach we use is to combine and apply three perspectives to a specific instance of digital industrial policy: 1) international relations, 2) national or EU competitiveness, and 3) business economics and business strategy (Figure 5).

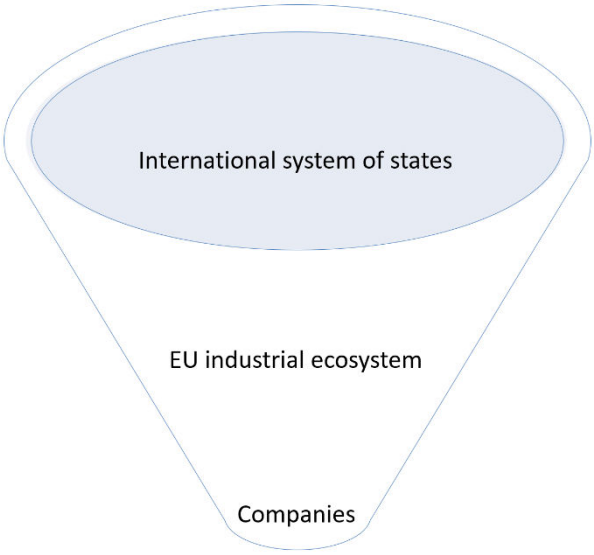


Figure 5: Three perspectives on digital industrial policy

The key objects in these three perspectives are, naturally, the **company** or firm and the **state**. At the level of international relations, we find the international system of states (a term commonly used in political sciences). At the level of competitiveness, we find industrial ecosystems comprising the relevant economic actors including companies and the state. Other notions that are frequently encountered in literature on economic governance are markets and networks (and some add to this: platforms). We address these here as objects in the industrial ecosystem (see Figure 10 in Annex I). At the level of business economics and business strategy we find individual firms.

As a first step, we analyse a concrete situation, in which 'digital' and industry play a role, in terms of these three perspectives. As a second step, we relate the three perspectives to each other (Figure 6). For instance, how do state aid or R&D subsidy, as policy actions aimed at individual companies, impact national competitiveness or international relations? And conversely, as another example, how does an international partnership agreement impact the value chain of individual companies?

This approach is relatively novel. Rarely has industrial policy been approached from the *combination* of these three perspectives even if there is increasingly a call to do so[24]. The approach allows use to analyse policy action with expert insight and develop 'smarter' policy. Yet, it is a start only. It does not yet provide a general model that relates the dynamics at each of the three levels. Such a model is an ambition that is beyond the scope of this report (if feasible at all).

[24] (E. Cohen, 2022).

Generally, as we would do for any industrial policy, the analysis needs to consider **completeness**, **consistency**, and **impact** of policy measures. Specifically, as this concerns *digital* industrial policy, we also must check if and how the 4S of digital (speed, scale, systemic, synchrony) are addressed.

'Completeness' is not only about the traditional industrial policy toolbox but also about related policies, - and given the interest in strategic autonomy, - notably the international policy toolbox. 'Consistency' means alignment or misalignment of objectives, such as strategic misalignment between company and state interests. 'Impact' means the contribution of policy actions to the objectives of each of the three perspectives. Here we can identify whether these are positive or negative and, if possibly, size these contributions.

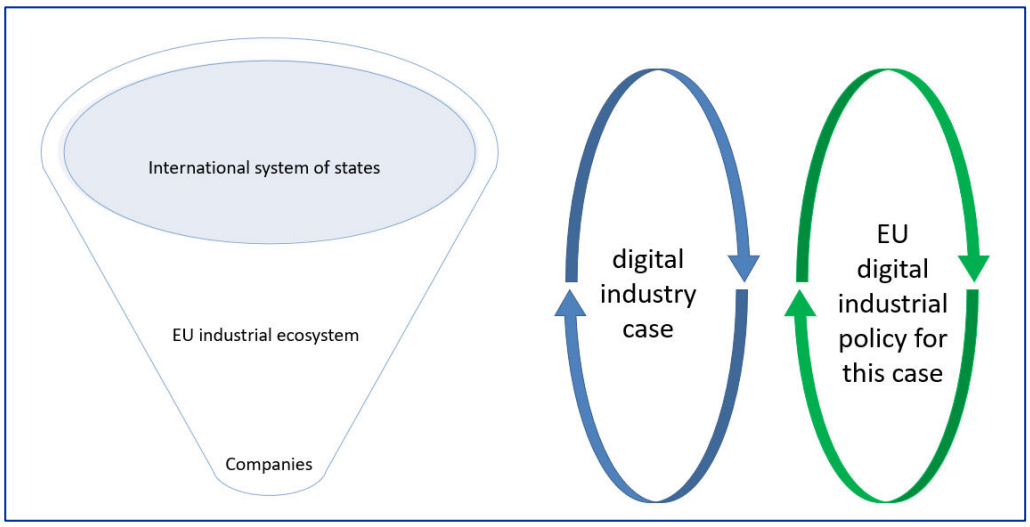


Figure 6: Analysis approach

Assuming the user has extensive knowledge of a specific situation, the analysis framework helps to identify and assess impact or other aspects of policy. We start from the business level, go to national competitiveness and then to the international relations level. As an example: with knowledge of technology, actors, markets in digital identity, we can envisage developing digital industrial policy for an EU industrial ecosystem in digital identity which – in theory – should enable viable business, strengthen EU competitiveness, and contribute to strategic autonomy. Analysing the contributions to this hierarchy of goals, we keep an open mind on whether these are limited to the digital identity ecosystem, or useful for a wider industrial ecosystem. The digital identity case will be developed in a next chapter.

Business strategy and industrial economics

Business strategy and industrial economics spells out the reasons for companies to engage in specific business models[25] and business relationships with partners and suppliers. Companies are seeking turnover, profit, market share etc. Which business alliances to establish is a strategic choice problem for reasons such as to reduce transaction costs, get access to resources, or get access to markets or innovation. We must understand these motivations of companies since they play a role when trying to influence company behaviour with industrial policy. In summary, key notions that we use in assessing digital industrial policy, from the business strategy and industrial economics perspective are:

1. Company performance
2. Strategic choice in alliances
3. Company's relations to government / state.

Industrial Ecosystem and Competitiveness

Industrial ecosystem and competitiveness theories address the industrial ecosystem, competitive forces, value chains, markets (and market failures), networks, innovation, national systems of innovation and innovation clusters, investment, industrial transition, and digital platforms as markets. This is an extensive field of study and practice[26], from which we use as an entry point for the analysis of industrial ecosystem and national/EU competitiveness Michael Porter's diamond model (see Figure7[27] and Annex I: additional theoretical background).

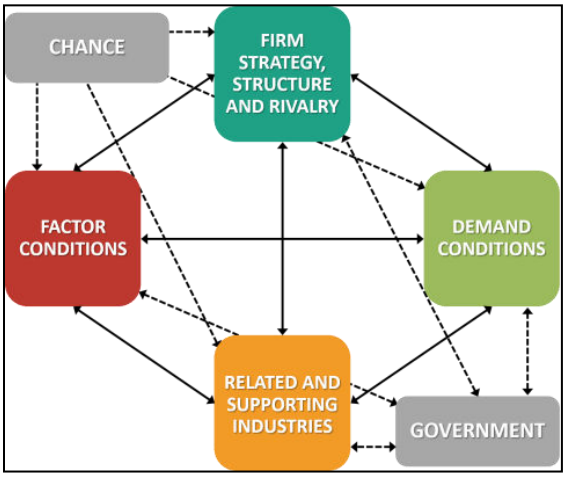


Figure 7: Porter's Diamond model for national competitiveness (sources: see footnote 27)

The focus is competitiveness, but other foci or objectives can also be considered as mentioned above. Sovereignty can be amongst those. However, although long-term national competitiveness is undoubtedly part of national sovereignty, sovereignty arguments are rarely invoked in industrial ecosystem analysis, unless defence is considered as a component in the ecosystem (and even then

[25] Business model literature is vast. For an introduction see (Nielsen & Lund, 2014).

[26] See e.g. the World Economic Forum Competitiveness Index and research on national competitiveness (Delgado et al., 2012), Michael Porter's Diamond Model, Scott Stern's work on Industrial Clusters (Delgado et al., 2014), and the general analysis of European industrial policy by (Bianchi & Labory, 2020), and furthermore (Freeman & Soete, 1997), (Dosi et al., 1988), (Kenney & Zysman, 2016), (Codagnone et al., 2018).

[27] (Porter, 1990) and (de Bruin, 2018) based on (Porter, 1990).

with the warning that a focus on *national* defence can become a barrier to success in global markets).

These theories provide a very strong and systematic emphasis on strategic analysis. They also come with usable models parties involved in an industrial ecosystem and their roles[28], including the roles of government. Care has to be taken suggesting that government would have the required information, planning and executing capabilities. Neither should there be a belief in the power of planning or in 'one best way'

In summary, key notions that we use in assessing digital industrial policy, from the industrial ecosystem and competitiveness perspective are:

1. Companies: actors, factors, market conditions
2. State: government roles as buyer and regulator
3. Relations between actors in the ecosystem.

International relations and geopolitics

International Relations and Politics addresses geopolitical strategy, global governance, international political economy and what is sometimes called geo-economics. International relations studies had until recently relatively few contributions to make to industrial policy. Certainly, most industrial policy is relevant internationally. For instance, it could lead to WTO complaints. However, this is a consequential rather than an *ab initio* situation. The latter would be when international relations and geopolitics is a strong factor in driving industrial policy. Indeed, this is where we find ourselves today. Leading industrial policy thinkers talk of an inflection point towards a new approach to industrial policy[29].

Digital industrial policy is the trailblazer of a new approach to industrial policy. In several ways this is different from the past. First, the Washington Consensus[30] is no longer a consensus. In fact, it is increasingly rejected around the world (Rodrik, 2022). Second, key notions of international relations start to be made explicit as drivers of industrial policy. In the USA economic security, that is, economic strategic autonomy[31], is already one-to-one with national security in the relation with China. Public funding, tax benefits and state aids for downstream activities such as manufacturing are considered to be justified, even in the USA (e.g., in the CHIPS and Science Act[32]). In Europe, the lucid writing of (E. Cohen, 2022) introduced us to the notion of *souveraineté industrielle.*

Third, understanding is growing that technology and geopolitics shape each other, in both directions[33]. This is the theme of the rising field of techno-politics (Eriksson & Newlove-Eriksson, 2021). Blockchain, quantum computing and readily available technology for cyber-attacks as well as the large cloud and digital platforms unsettle state sovereignty. Technology, in a fundamental way, affects the

[28] For instance the OECD has used these models to analyze the national competitiveness of Finland, Mexico, and several other countries.
[29] E.g., Aiginger & Rodrik (2020), E. Cohen (2022), or Rodrik (2022).
[30] See footnote 9 for definition.
[31] The term is used in the same way as digital strategic autonomy or financial strategic autonomy, see footnote 3.
[32] (US Congress, 2022).
[33] More generally, technological construction and social construction (sovereignty, public governance, but also industrial ecosystems, markets, firms) are in a closer and mutual interrelationship than often thought, see references later in this report.

international system of states as new actors such a large tech companies but also rogue states enter the play. 5G/6G and IoT technical architectures and standards are serious concerns for national security and the technical architecture of the internet itself has *de facto* been fragmented to reflect regional blocks. This shows that technology is also being fundamentally shaped by geopolitics. The interplay of technological and social construction of sovereignty has been analysed by (Timmers, 2022a). An illustration relevant here (see the cloud case) is that sovereignty concerns about access to sensitive data can be alleviated by new encryption approaches. Likewise, concerns about security can be reduced by blockchain-enabled distributed security and quantum communications. At the same time, a new threat to sovereignty is quantum computing as it may crack pre-quantum encryption.

This emerging change of thinking has not yet led in academic literature to authoritative models for the combination of international relations, industrial policy, and digital technology. Rather than waiting for a comprehensive framework, we can move ahead here by analysing key notions of industrial policy from an international relations perspective, such as markets, supply chains, technology alliances[34], standardisation[35], or industry platforms. Conversely, we can analyse, from an industrial policy perspective, key notions of international relations, such as security, strategic autonomy, dependencies, and resilience. Moreover, we look at digital technologies (speed, scale, systemic, synchrony) from an international relations perspective and vice-versa.

[34] (Timmers, 2022b).
[35] Geopolitics and the European standardization system is also analysed by Baron & Larouche, (CERRE, forthcoming).

4. APPLYING THE THREE PERSPECTIVES TO SELECTED CASES

The three perspectives have each their own theoretical foundations. As we will show, they are each useful to analyse industrial policy. What is missing is how they relate to each other. There is little theoretical work yet. What we do here is link them through two of the terms that they have in common: company and state. Their interactions manifest themselves in business models, supply and value chains, industrial ecosystem, national competitiveness, alliances, strategic partnerships, the international system of states, and geopolitics. These are all key notions for our DIP. We therefore follow a 3 + 1 analysis: three perspectives plus relationships between the perspectives.

4.1. Semiconductors

4.1.1 General

Semiconductors are the chips that we find in most electronic equipment. The semiconductor value chain is very complex. It ranges from fundamental research of materials and their electronic components, to how to manufacture them, the design of computer logic, preparation of the many materials (silicon, gases, rare earths, chemicals) needed for production, the manufacturing where chips are etched onto silicon wafers, cutting of wafers, wire-bonding, packaging, and testing. Most attention goes to the so-called fabs that produce the wafers, use multi-million-euro lithography machines, in clean rooms. These fabs can cost up to 20 billion euros. But all these other steps are indispensable too. Most importantly, often there is a dependency on a few of even just one supplier and it is very difficult or impossible to replace them by alternatives. All of this makes supplier diversification or building homegrown producers hard. The high level of chokepoint dependencies can lead to supply shocks caused by industrial incidents (e.g., factory fire, Japan 2020), war (Ukraine 2022), or securitisation of supply (USA, from 2018)[36]. In addition, and even more than the other cases in this report, there is a high dependency on intellectual property (IP) which is generally protected by patents or 'company secret'.

The market is projected to grow fast, even if it is highly cyclical, to about 1000 billion USD by 2030 from today's 600 billion USD.

[36] Chip War by Miller (2022) provides an insightful analysis of semiconductor ecosystems and market dynamics around the world.

4.1.2 Analysis of situation

Company level – fabs need huge capital, land, skilled labour; specialists SMEs need talent, partners

This is a very mixed industry, comprising both companies with huge Capex (fabs) and highly innovative smaller companies whose valuation can suddenly skyrocket. Some companies are purely IP-based such as those in chips design. Patents and brains are their main asset. There is significant M&A activity, which is increasingly scrutinised and sometimes blocked on national security grounds[37]. This can also include that governments take a financial participation in order to pre-empt foreign takeovers[38]. Fab investments have long lead times (3-10 years) and the industry has a high cyclicity.

For any type of company, it matters in which environment they are placed. For instance, fabs require huge amounts of electricity and water as well as highly tuned manufacturing skills. Therefore, the supply, reliability, and price of these factor conditions are key competitive conditions and whether or not to influence them should be part of industrial policy reflection.

Design and other specialist companies need the supply of highly skilled knowledge workers, often coming from other companies in related business and from top universities, that is, the intellectual environment is another key factor condition. No company can master all the thousands of steps in the semiconductors' value chain. Therefore, companies need partners, often many, and this notably holds for the larger companies that operate fabs. For binding and packaging, companies depend on relatively low-skilled manual labour, so price of labour matters.

Companies will carefully consider these conditions. Telling are the complaints of TSMC about lack of skilled workers in manufacturing for its plant in Arizona[39], and the fierce debate about the strategic orientation of India's semiconductor plans, namely whether to cover the whole value chain, or to rather focus on their low-skilled labour and design competitive advantages[40]. Industrial policy must cater for the different company types.

National competitiveness level – key determinant is the structure of the industrial ecosystem

Often it is argued that semiconductor industrial ecosystems must have a strong complementarity of buyers and fabs, and R&D with fabs. In Taiwan this is the personal computers/smart phones – fabs relation. For EU fabs it has been argued that this would be automotive, industry 4.0, edge computing, and telecoms. For India it would be a very broad set of industries (Reed, 2022). Does the argument really hold? Is a globally open, trading economy an alternative? An example could be Singapore, with several fabs but less in terms of user industries. It has also been argued that EU's user industry does not need the most advanced chips[41] but this is contested by other analysts and voices from industry[42].

[37] In the EU this can be done in several countries (e.g., France, Germany) under national legislation or under the 2019 Foreign Direct Investment Regulation. In November 2022 the German government blocked Chinese take-overs of two semiconductor companies.
[38] An example is the Dutch government taking a share in Smart Photonics (Thole, 2020).
[39] (Yu et al., 2022).
[40] (Reed, 2022).
[41] (Kleinhans, 2021).
[42] (Accenture, 2022; Kearney, 2021; Lambert, 2021).

For instance, EU's consumption of leading edge semiconductors (below 5 nm in 2030) is projected by (Kearney, 2021) to grow much faster than mature and advanced semiconductors, that have a larger node size (Figure 8).

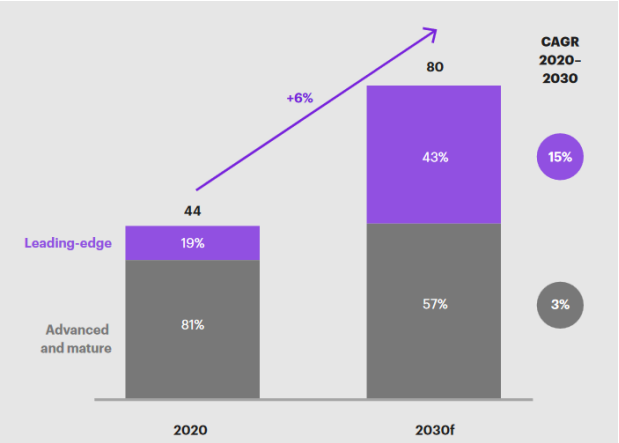


Figure 8: EU consumption of semiconductors

Past long-term government planning can pay off. Taiwan is the leading example, where government planning and financial and R&D support (to achieve R&D expenditure as high as 3.4% of GDP), has been very significant for the success of TSMC, Acer, Asus, etc. Moreover, market regulation affecting user-industries can have a large impact, e.g., companies such as Infineon and NXP benefited much from EU's automotive safety regulation. Comparable market regulation is rare across the world, except for America-First and China-First obligations. These straddle the line between stimulating national competitiveness and geopolitically motivated restrictions.

Skills of different types are crucial. Fabs require abundant and very sophisticated manufacturing skills. Upstream, control of fundamental and applied research skills, gives a say in shaping the next-generation industrial ecosystem such as for quantum technologies - in which the EU has a strong position - or for accelerated design in which on its turn the USA is strong[43].

Public policy includes massive investment support across the world (USA, China, EU, India, Taiwan, South Korea, Japan), while, generally, R&D support is included too. Only in China and Taiwan did public policy since a long time include talent and skills development. In the USA, only recently policy starts addressing the grave concerns about the lack of domestic skills. Taiwan systematically addresses institutional learning, inside and between government and industry as Japan also did in the early days. However, in other countries and regions institutional learning is virtually absent. Public procurement policy, except for defence and military, is absent as a public policy instrument.

In the EU, semiconductor policy initiatives undertaken since 2014 did not manage to put a halt to the erosion of manufacturing market share of the EU. Neither did they provide a buffer to the 2021-2022 crisis of semiconductor shortages. These pre-2022 initiatives did not address the full ecosystem in terms of actors and activities (from R&D to manufacturing, to skills, etc.). The EU situation is to change radically with the EU Chips Act which was proposed in February 2022 by the European Commission, and which is discussed below.

International relations level – clash of geopolitics and semiconductor fundamentals/economics

Semiconductors need a wide range of inputs and materials including rare earths. This leads to critical dependencies between countries. The economics of semiconductors also pushes for locating activities

[43] For instance, reducing time towards 'tape-out', i.e. ready for manufacturing (Berkeley Engineering, 2021).

where factor conditions are best, e.g., packaging in cheap-labour countries. This increases efficiency but also leads to resilience risks, cf. the chips supply chain shock. Value chains are managed with the help of complex ICT systems, which in turn leads to security risks, as illustrated by the concerns raised since the SolarWinds incident in ICT supply chain security[44]. It also leads to dependencies between countries that are in different geopolitical blocks. Rising geopolitical tensions between blocks, notably between USA and China, clash with the economic supply chain logic. These tensions translate into two types of public policy initiatives that aim to:

1. Reduce dependencies, systematically or to reduce vulnerability to supply shocks;
2. Deny access to critical supplies in order to constrain or hamper a geopolitical competitor.

The first type of public policy initiative which includes diversification of suppliers, replacement innovation, and stockpiling. It often goes under the heading of resilience. However, when the objective is long-term import substitution it is about strategic autonomy and sovereignty.

The second type of action can range from reducing access to rare earths, production equipment, chips designs and design software through export restrictions to conditional investment support. In international relations jargon this is referred to as the 'securitisation' of semiconductors.

Clear examples of both types of actions are in the 10-year China ban of the US CHIPS and Science Act[45], the USA's Entity List; and in China's chokepoint analysis[46] which identifies a whole range of actions such as supplier diversification, support to domestic industry, buying foreign companies or IP, and IP copying. Western intelligence also reports large-scale industrial espionage by China. China's goal is to meet semiconductor needs for 70% by 2025 by domestic production, up from 16% in 2020.

Worldwide, all public policy for semiconductors targets fabs (the huge companies) and the knowledge/R&I basis. Some public policies, e.g., in China, target wider dependencies such as design software and lithographic equipment. Few public policies target skills. None – except Taiwan–s - are about institutional learning. Public policy instruments include investment support-with-strings-attached (EU: resilience; US: non-China, CN: government board-level influence); limited regulatory intervention (EU: resilience, sustainability), public R&D prioritisation (EU: quantum), standardisation (EU/US in the Trans-Atlantic Trade and Technology Council).

The semiconductor industrial policies around the world are unavoidably leading to clashes over:

- investments, e.g., subsidy races
- patents, e.g., patent squatting and patent flooding
- talent, e.g., working conditions
- rare earths, e.g., exclusive exploitation rights.

[44] SolarWinds is a Texas-based company that fell victim to a sophisticated cyber-intrusion, attributed to an actor that is likely Russian in origin. Malware was inserted into trusted third-party network management software (of SolarWinds). The intrusion was discovered in 2020 but had likely been going on for over a year. Very many companies were affected – several in the semiconductor sector - and governmental departments, including in defense and security, see (Senate RPC, 2021).

[45] (The White House, 2022).

[46] (Murphy, 2022).

Such clashes are caused by both competitive rivalry between national/regional ecosystems and by the 'weaponisation' or 'securitisation' of semiconductors in the context of geopolitical rivalry or even war.

4.1.3 Analysis of EU semiconductor policy

Below we provide the most salient elements of EU semiconductor policy, namely the EU Chips Act[47], from the three perspectives mentioned before and analyse interlinkages.

Company level

EU policy responds to the needs expressed by fab companies for financial support and favourable investment conditions. It is not clear, however, whether the voice of companies has been heard in the past and is currently consistently taken into account. An unanswered concern is that the EU budget appears far below the investment needs to achieve the target of doubling the EU's production share of advanced semiconductors by 2030, as expressed by (ASML, 2022) and (NXP, 2022). Paradoxically, while possibly the EU invests below what is needed, the world as a whole may be over-investing, risking to create a chips glut by the time new fabs become operational, possibly exacerbating the already risky boom/bust cycles of the semiconductor market as suggested by (Waters, 2022).

Moreover, a range of criteria (financial incentives, skills levels, local ecosystem, energy prices, etc) are input to the decision-making of fab companies to choose between the EU, the USA, Korea, India, Japan or China (if they must do so). There is a lack of clarity about these criteria and the related decision-making and how these evolve with changing circumstances. The EU Chips Act needs a rolling impact assessment on investment strategies, investment needs, and effectiveness of investment. Legislation and policy should then be able to be better prepared than is the case today for swift adaptation to changing circumstances. That is, legislation, based on the rolling impact assessment can foresee flexibility within bounds (inspiration can come from the specific flexibility in the EU Chips Act to handle semiconductor supply crises). In the EU, legislative mechanisms can be Delegated or Implementing Acts. Alternatively, by anticipating possible changes, fast-tracking modification of policy in force may more likely be feasible[48],[49].

A risk at geopolitical level are subsidy races. The USA and EU are aware of that and seek to avoid it via the trans-Atlantic Trade and Technology Council (TTC). The Paris-Saclay TTC Statement of May 2022 mentions the mutual intention to not get into WTO disputes, but the mechanisms remain to be clarified and put to the test. Moreover, subsidy races are not limited to the EU and USA but are also possible and even likely in the RoW, notably, Taiwan, South Korea, Japan, India, and Singapore. It remains to be seen whether there will be a subsidy race with China, despite the appeal of huge

[47] A more extensive description of EU semiconductor policy (the EU Chips Act) is in Annex II.

[48] This could be argued to become a contribution to the EU's Better Regulation approach.

[49] A rolling impact assessment would be an ad-hoc or regular assessment of the impact of changes in the assumptions of the ex-ante impact assessment of an EU policy that is in force. Ad-hoc triggers can be major new policy initiatives of third countries (such as the USA CHIPS and Science Act), significant economic changes (such as the 2022 electricity price shock that may strongly affect fabs), technological/engineering breakthroughs, or critical foreign direct investment activity. Regular re-assessment would be more frequent than the standard review clause in EU legislation (in the case of the EU Chips Act this is 3 years). Scope and allowed consequences of a rolling impact assessment likely must be fixed in advance in order to maintain both regulatory certainty and regulatory relevance.

government subsidies, given that the USA CHIPS and Science Act appears to seal off the China-route for companies with advanced chips facilities (many of whom also depend on the US market).

Subsidy and trade conflicts between the USA and EU are also showing up in other domains while such conflicts can well spill-over between domains. In the domain of green investment, the USA Inflation Recovery Act advantages USA car manufacturers, to the dismay of the EU. Here too the strategic objective of the USA is to become independent and thus strategic autonomy and geopolitics play a role. We should anticipate that critical materials initiatives (announced by the EU and the USA and already pursued by Korea) likewise will be touched by geopolitics, which could open yet another battlefield on state aid and subsidies.

Therefore, it is reasonable to say that there is a risk of inconsistency in the EU policy between the company and the geopolitical levels. Despite the fact that the EU Chips Act was triggered by geopolitics[50], a fully developed geopolitical approach to subsidy races is missing in the EU Chips Act, though work in the trans-Atlantic relationship may at least partially address this. Likely similar problems will manifest themselves in other policy domains in the quest for strategic autonomy and/or resilience.

However, this is also an opportunity for anticipatory policymaking. Namely, to learn from cooperatively resolving semiconductor issues in the TTC and anticipate to broaden dispute resolution and mediation mechanisms in order to involve a variable configuration of states. Work in the TTC and experiences (positive and negative) from the WTO[51] can therefore provide guidance. It cannot be the WTO to take the lead here given that its membership extends well outside the group of countries mentioned above. Possibly preparing for handling subsidy disputes in strategic autonomy areas can be on the G7 agenda.

Smaller specialist companies are served in several ways, notably through partnerships in the EU's Industrial Alliance on Processors and Semiconductor Technologies that is part of the EU Chips Act, and for R&D support and R&D talent through the Horizon Europe programme and the support for skills hubs. In the policy it is not clear, however, whether the voice is heard of smaller companies. The lack of consultation mechanisms increases the risk of inconsistency between the interests of individual companies and the direction pursued for the industrial ecosystem as a whole.

Finally, for individual companies the lack of obligations for intellectual property (IP) control[52] or restrictions on international business relations such as on foreign direct investment or mergers and acquisitions, may lead to inconsistencies with geopolitical interests, even more so where the US CHIPS and Science Act and Chinese policy do have such restrictions. The current EU FDI Scrutiny Regulation addresses co-operation and exchange of information between EU Member States when an FDI cases

[50] The European Commission mentions the semiconductor supply chain disruptions since 2020, massive investment for "Made in China 2025", the then-imminent US Chips Act, announced investments in Japan and South Korea, and generally, geopolitical tensions (*A Chips Act for Europe*, 2022).

[51] (Klabbers, 2021, p. 306).

[52] IP control in the sense of strategic autonomy, that is, IP ownership or at least a decisive voice on what happens with IP (such as a golden share arrangement). IP control is in this document used interchangeably with IP protection.

occurs (i.e., ex-post) but neither address ex-ante IP protection (i.e., IP control, see footnote 52) nor more forceful measures than coordination[53]. Not addressing IP matters leads to a lack of reciprocity enabling to 'negotiate from a position of strength'[54]. It is easier to raise the issue of IP protection than to solve it. The starting point could be to include an IP protection scrutiny when receiving EU or national subsidies. Though this may sound similar to existing security scrutiny (as in the EU Horizon R&D programme), it would be less imposing as it could be limited to record potentially strategically sensitive IP developments and impose a requirement to report the initiation of FDI. This is a *quid pro quo* to receiving public support. As a rather lightweight approach this will not protect all strategic IP. Upping the ante, but not realistic, would be to pro-actively establish a register of strategically sensitive IP developments with FDI reporting obligations.

National competitiveness/industrial ecosystem level

The EU Chips Act, through its Chips Joint Undertaking and Industrial Alliance on Processors and Semiconductor Technologies, strengthens the industrial ecosystem by connecting large to small companies. The EU Council emphasises that the supported fabs (Open EU Foundries and Integrated Production Facilities) should have positive spill-over effects on the EU semiconductor value chain in terms of increasing resilience and skills[55]. It also steps up EU risk capital funding, but it is not clear if this will meet needs and can compete with foreign venture funds. Moreover, there is no flexibility adjustment mechanism foreseen to increase funding if needed. The aforementioned investment rolling impact assessment should address this.

It may be less evident in semiconductors whether government can also be a substantial buyer. Nevertheless, since government is a significant procurer in public infrastructure and services (transport, logistics, water works, defence) it could include semiconductor requirements in public procurement.

Of concern is that the EU skills plans are weak, whereas lack of skills is increasingly becoming a challenge. The situation is similar in the USA and reportedly in South Korea too[56]. On the contrary China has a long-term and large supply of STEM graduates[57]. Therefore, a talent war between the USA and the EU would only be self-destructive in the face of competition with China. In an interesting study for FEPS, (Anderson, 2022) showed that brain drain from the EU to the USA is significant, the EU losing 15% of its PhDs (in the field of AI). Buying talent also happens through takeovers notably by big tech firms (estimated to be the purpose of more than half of their acquisitions). This may feed into the creation of tech/talent hubs, a self-reinforcing dynamic to increase the prospect of intellectually and financially rewarding careers. Semiconductor companies such as ASML undertake extensive efforts to improve housing for prospective employees. The EU does promote the hub concept (generally in digital technologies and specifically also in the field of semiconductors), but can do more to share best

[53] (European Commission, 2020a)
[54] (Breton, 2022b).
[55] (Council of the European Union, 2022).
[56] (Ji-hyoung, 2022).
[57] (Zwetsloot et al., 2021).

practices in creating attractive talent hubs[58]. (Anderson, 2022) recommends integrated policies addressing quality training, immigration, programs for women, tax incentives for small firms, housing, and transport. Such joining up of policies will not be possible without political and administrative leadership inside governments.

There is also little regulatory punch in market access conditions for sustainable production. One could argue that such regulation could lead to retaliation, WTO complaints, and limiting global reach.

This national competitiveness/industrial ecosystem level could be consistent with an overall global partnership approach but appears inconsistent with the actual geopolitical approach of the EU Chips Act, namely, as (A Chips Act for Europe, 2022, p. 11) states, of a strategic partnership *in particular with like-minded partners*.

A relatively new intergovernmental industrial policy instrument must also be mentioned here and also in the cloud case below: Important Project of Common European Interest (IPCEI)[59]. These are projects funded from national budgets, involving at least four EU Member States, bringing together knowledge, expertise, financial resources, and economic actors, in order to address important market or systemic failures or societal challenges that could not otherwise be addressed[60]. IPCEIs can benefit from state aid. While reportedly slow to come to fruition and susceptible to significant delays in their execution[61], the IPCEI instrument is praised for creating leadership in strategic value chains and striking an acceptable compromise with competition policy in the pursuit of strategic autonomy[62] but also criticised as being opaque and ill-defined[63]. In our context it is important to understand whether IPCEIs are consistent and synergetic with EU-level digital industrial policy. An extended micro-electronics IPCEIs has been launched which appears to complement the EU Chips Act. However, by definition IPCEIs are more exclusive in participation than EU policy. This may enhance political sensitivities about involving (or not) all Member States in such a strategic industrial development. Unbalanced intra-EU development tends to raise fears about fairly sharing related EU financing (in EU jargon, *juste retour*). In particular, this may play a role for semiconductors, given geographic concentration in just a few countries of fabs and design centres. Nevertheless, the revised micro-electronics IPCEI involves now 20 Member States up from just 5.

[58] The EP rapporteur on the Chips Act is urging for more action on skills related to the envisaged semiconductor Competence Centres (NICA, 2022).
[59] The IPCEI instrument exists since 1957 but has only recently been invoked, for batteries, hydrogen, micro-electronics, cloud, and health.
[60] (European Commission, 2021d).
[61] (Stefan Sagebro, 2022).
[62] (E. Cohen, 2022).
[63] (Poitiers & Weil, 2022).

International relations / geopolitics

On the supply side, the EU is open to but also dependent on investment from US, Taiwanese, and Korean companies. Conversely, the EU generates significant business in China, such as for the lithographic equipment of ASML. This means that the USA's China-restrictions, which are motivated by American national and economic security, are likely to affect EU business. Moreover, a subsidy race between the USA and EU may be triggered unless this is mitigated. EU policy does not yet have a clear approach to avoid subsidy races with Taiwan or South Korea or Japan, and some but not clearly articulated approach with the USA, in the TTC (see, however, the positive potential of the TTC mentioned before in the section on the company level analysis). There is also no approach to IP protection (IP control) and export controls. There is no protection against take-overs by USA or others of small but promising EU companies, even if these have been benefiting from industrial ecosystem policy such as Horizon Europe funding. The EU must consider an early-stage golden share policy.

The lack of such international policy interventions creates uncertainty for the industrial ecosystem and even for individual companies, notably for fabs. That is, the policies need to be completed and made consistent between the three levels of international relations, EU competitiveness, and business strategies.

The EU Chips Act is explicit on dealing with chips supply shortages. However, what is missing is an analysis of remaining dependencies, such as rare earths or specialised components, and policy action to deal with them notably in geo-political perspective, i.e., an analysis of geopolitical risks. A European Critical Raw Materials Act has been announced by (von der Leyen, 2022). It is necessary to complete the EU's geopolitical chokepoints analysis and complement this with industrial policy action. Although such analysis could be performed at company or ecosystem level, the focal point here is the geopolitical level even if the implications of such policy are at ecosystem and company level as is evident from the earlier quoted Chinese chokepoints analysis (e.g., supporting specific domestic companies, additional R&D into substitutes, etc).

Remarkably, the EU Chips Act is rather lightweight as regards pro-active outreach to likeminded partners. We can contrast this with the active USA outreach to Japan, Taiwan and South Korea, forming the Chip 4 Alliance. The Act also does not address international standards or other global commons such as environmental protection. The international relations dimension of the EU semiconductor policy is to be further developed in order to progress global partnerships, standards and sustainability. In first instance this seems to fit largely with the geopolitical level though it may contribute to the EU's industrial ecosystem for at least two reasons: standards may get linked to internal market regulation; and if partnerships are constructed to have mutual dependencies, i.e., reciprocity, this asks for specialisation within the domestic (EU) ecosystem.

In conclusion: as a digital industrial policy the EU semiconductor policy is a leading example in terms of range and concreteness of policy actions. Nevertheless, the analysis reveals significant gaps and some inconsistencies. This asks for further policy action in order to connect from company to ecosystem to international level for greater completeness and consistency, and thereby greater impact.

In particular, the EU Chips Act needs a regular 'stress-test' or rolling impact assessment in geopolitical perspective to ensure that it sufficiently consistent, complete, and impactful– which it is not today.

The analysis is summarised in Table 1.

Table 1: Gaps and inconsistencies in EU semiconductor policy

Risks	Gap or inconsistency	Proposed policy action
Geo-political developments and foreign chips plans	Lack of geo-competitive adjustment	Rolling impact assessment on investment/funding
Investment needs	Funding gap to achieve the EU's 2030 production share targets	Rolling impact assessment on investment/funding
Subsidy or other trade conflicts, uneven playing field amongst the 'like-minded'	No plan to deal with subsidy races or potential trade restrictions	Co-operation on subsidy or trade restraints with US (in TTC) and other countries
SMEs get side-lined	Lack of SME voice	Include SME platform in Alliance on Processors and Semiconductor Technologies
Intellectual property (IP) gets extracted	No IP control obligations	IP control obligations linked to EU funding
Foreign take-overs	Limited guardrails against foreign M&A and other forms of investment	Develop governmental shareholding policy with EU Member States
Foreign chips policies bypass EU Chips Act	EU chips policy gets decoupled from chips policy of other powers	Develop international dimension of EU chips policy

4.2. Cloud and Platforms

4.2.1 General

Cloud has become an essential infrastructure for the economy and society. In its basic form it consists of remote storage of data and remote access to computing also called infrastructure as a service (IaaS). This can be enhanced by platform as a service (PaaS) which can be seen as providing a complete remote operating system and software environment. On top of that, cloud services can offer complete software environments and applications. These may include website hosting, data processing and analytics and AI. They may also provide application suits from word processing and emailing to customer management or telecommunications support such as bringing 5G functionality into the cloud (virtualisation), also called also called software as a service (SaaS). Cloud providers offer a rich and ever richer set of ICT functionality. Cloud offers scalability, availability and security that is not easily realised by an individual company, certainly not by SMEs with little inhouse ICT expertise. It has become a natural reflex to ask: 'can we run this in the cloud?'.

Cloud runs in data centres which require ever larger investments to grow scalability. Electricity consumption and environmental sustainability are challenges[64]. Large cloud operators can increasingly outcompete smaller ones thanks to their financial buffers against rising electricity prices[65]. Ever larger data centres and ever-expanding IT expertise, e.g., in security and AI, bring important economies of scale. From this perspective it is understandable that the industry is highly concentrated.

Cloud services in the EU are dominated by Microsoft, Amazon, and Google, and worldwide by these tech giants plus large Chinese players Alibaba and Tencent, with Huawei being a runner-up. Google is a special case as it can combine the virtual and the physical world, being also one of the two dominant players in the smartphone market with its Android mobile operating system which is tightly coupled to Google cloud. Another such example is Huawei which runs a smart cities platform combining devices/sensors and cloud that is making significant inroads into Europe. Google and Meta (Facebook) command also large physical communications infrastructures (cables), etc. and encroach on traditional telcos[66]. A number of cloud providers also run an online platform, that is, a rich environment for two-sided interactions and transactions such as a social media platform or online retail platform or personal communication services such as Whatsapp. Very large platforms may also run their own cloud services with related data centres, e.g., Facebook.

The large players benefit from a virtuous cycle that combines growing scale, growing functionality, with growing profits and thus growing investment capacity. This gets magnified by customer lock-in. Since cloud interoperability, data and application portability are not naturally put in place by the large players or made difficult by practices such as charging egress fees[67], many smaller cloud providers are struggling to capture market share. Issues that have been reported include unfair contract conditions that are effectively creating a lock-in (such as making price comparisons difficult), predatory take-overs and other forms of abuse of dominance by the large players[68]. Countering these market failures is one of the aims of regulatory intervention, which in the EU is by means of both ex-ante regulation (EU Digital Markets Act, EU Data Act) and ex-post competition action (competition cases).

Concerns are expressed by governments and civil society about the power of these large players when it comes to control of data security, infrastructure security, identification, and currency. These concern the core of sovereignty, namely securing sensitive data, continuity of public services, sovereign identity (national ID) which is the basic government-citizen link, and control over the banking system. Gradually it has become clearer that consequences of foreign dominance are that a foreign government can force access to data (USA Cloud Act, China Data Act) and that there is a growing dependency on large foreign cloud companies when it comes to ensuring national continuity of service[69]. Moreover, with data analytics and user identification also under their control, cloud and platform providers can potentially steer citizen behaviour or allow for manipulation. When this affects

[64] (Banet et al., 2021).
[65] (van Wijnen et al., 2022).
[66] (Stocker et al., 2021; Voelsen, 2019).
[67] Charging for exiting the cloud platform.
[68] (Vodafone, 2022).
[69] The Snowden revelations unleashed many discussions on relationships between national security agencies and major software companies. These continue until today but now in the context of the stockpiling of vulnerabilities by China (Dobberstein, 2022).

democracy and societal participation, it becomes yet another sovereignty concern[70]. These large cloud companies may then become target of both cloud and AI (or data ethics) strategic autonomy policy.

Added to these concerns is that the very large companies increasingly decide on the added-value from their data handling, such as AI-based services, locating the related jobs and knowledge away from where data originate. When data is seen as a sovereign asset (which is increasingly the case), deciding on the value-added is also seen as a sovereign right, i.e., a matter of control in strategic autonomy terms. This holds even if the country may not have the capabilities and capacities to create itself such added value. Adding up the concerns, we are squarely in the strategic autonomy discussion, strategic autonomy being defined here as having control, capabilities, and capacities (3C) in the interest of sovereignty. Clearly internal legitimacy of governments is at stake (does the government ensure that 'our' data and its value-added belong to us, as European Commissioner Thierry Breton expressed it[71]), as well as their external legitimacy (can foreign governments interfere). In several EU countries such as France and the Netherlands, the choice of government for foreign cloud providers has been criticised. Calls are increasing for 'a European sovereign cloud'.

4.2.2 Analysis of situation

Company level – strong concentration, sustained dominance of foreign large cloud/platforms

Cloud is dominated by foreign companies that are aggressively expanding in security, AI, and sector-specific applications. They follow what looks like a traditional monopolistic dominance approach but enhanced in the digital domain by network effects and lock-in due to lack of effective interoperability and portability. The huge valuations of these firms permit them to gobble up smaller value-added companies. At the same time, lots of innovative companies have sprung up around these few platforms.

Next to efficiency nowadays also security is at the top of corporate agendas. It is argued that cloud has massively improved productivity and security in user companies. Not only technical lock-in but also such strategic 'C-level' benefits give the dominant cloud providers a seemingly unassailable position. Competitors try to eat into their cake by stressing other values such as environmental sustainability (energy efficiency), data protection, interoperability and portability, and protection against foreign intrusion. Competition may also come from infrastructure providers, e.g., satellite operators, self-driving car industry, or telecom providers, though these too may get taken over by the cloud and platforms companies.

National competitiveness level – no domestic cloud ecosystem without strong EU providers

The EU is critically dependent on large foreign cloud providers. This leaves a hole in the EU cloud eco-system. There are three ways to address this: 1) build up strong domestic cloud providers; 2) accept the situation as is and compete with the large providers in value-added services to the cloud, such as AI/data analytics and trust services 3) offer a new cloud paradigm as alternative to centralised cloud, such as edge cloud. These three are – considered over time – not excluding each other. China has

[70] A notorious case is Cambridge Analytica.
[71] As reported by Politico (Kayali & Eder, 2020).

realised the first way but is also actively stimulating the two other ways. The EU policy in this respect is discussed below.

International relations level – cloud is geo-politicised and divisive even between like-minded countries
The large cloud providers have become less trusted by governments in the EU even if these governments have often little choice but to work with them. The dominance and economy-essential role of cloud providers has led to uneasiness with governments who feel they lose control on matters that extend well into their sovereignty, such as identification, access to data, contractual conditions, and critical infrastructure resilience. Chinese cloud providers are suspect for many, given the extraterritorial reach of the Chinese government and mistrust about its geopolitical motives. Between largely 'like-minded' partners, the EU and the USA, cloud has however, also gotten politicised, due to actual or presumed risks of extraterritorial reach of the US government (US Cloud Act) and the lack of governmental action against distortion of competition (contractual conditions) or democracy-undermining behaviour (content)[72]. Foreign dependencies raise concerns about resilience, security, and economic value creation and jobs.

There is limited cloud policy in the USA. On the contrary, China has an explicit and effective cloud policy, comprising data localisation, cybersecurity certification, and promoting large-scale cloud take-up such as in smart cities[73].

4.2.3 Analysing EU cloud policy

Here we summarise the most salient elements of EU cloud policy, analysing this at the three levels (company, ecosystem, international) and interlinkages between these levels[74].

EU Cloud policy is still evolving. An EU Alliance for Industrial Data, Edge and Cloud has been launched and the EU's cybersecurity agency ENISA is developing cloud security certification schemes. Extensive financial support for cloud R&D comes from the Horizon Europe programme and for cloud deployment from the Digital Europe Programme and COVID recovery funding (RRF). The large-scale GAIA-X initiative - initiated and supported by Germany and France and involving several other EU countries even if executed by the private sector -, develops and tests specifications for trusted and interoperable cloud and runs a large set of sectoral pilots. However, the EU does not yet have a single, comprehensive, and integrated cloud policy comparable to the EU Chips Act.

Company level – policy actions are about stepping up requirements in a fairly company-agnostic way
EU cloud actions as well as GAIA-X are provider-neutral. They do not squarely aim at any of the categories of cloud providers – European or not, large or small - nor are they specific to certain value-added providers. Rather, all of these companies are to be stimulated to advance generic requirements for security and interoperability and data protection. Political messaging on cloud is ambiguous in the EU. Some voices embrace EU cloud providers (or call for an EU sovereign cloud) while others, such as

[72] See f.i., for Cloud Act (NCSC-NL, 2022a) but also (NCSC-NL, 2022b), for distortion of competition (Vodafone, 2022), for democracy-undermining content, EU Digital Services Act and related impact assessment.
[73] (China Technology Forecast in 2025, 2020).
[74] A more extensive description is in the Annex II.

several Member States governments, maintain openness to the large foreign cloud providers. The Alliance has restrictive participation requirements based on national security grounds. Microsoft has set up what appears to be a competing European Cloud Alliance but other third country cloud providers have not joined (yet). The stringency of emerging EU security certification requirements has recently gotten politicised: a number of US cloud companies lobby against these as they fear to get excluded or be disadvantaged, having to also comply with the USA CLOUD Act. Finally, EU policy also does not seek to encourage consolidation of smaller European providers.

GAIA-X and the Alliance stimulate companies to engage in partnerships, mainly by lowering transaction costs for partnering, lowering interoperability barriers, promoting emerging standards, and easing access to sectoral markets. They thereby directly address company level interests.

Complementary or related EU policy may lead to new opportunities for companies in the cloud ecosystem. Examples are combinations of semiconductor and edge cloud, and combination of generic cloud with trust services, notably digital identity and digital wallet. In such cases it would be possible to prioritise EU companies, on the basis of security arguments. EU Cloud policy must consider the linking up with related semiconductor, digital identity, and cybersecurity policies.

The fact that public policy actions so far are relatively company-agnostic can be considered a weakness as smaller EU players are little protected against predatory or anti-competitive behaviour by the larger players (except for one piece of related policy, namely the DMA). It can also be considered a strength since it keeps options open when to define and structure the EU cloud industrial ecosystem.

National competitiveness/industrial ecosystem level – plugging the hole or not

EU policy actions and GAIA-X actions are quite comprehensive in ecosystem terms. All pure cloud players are stimulated, value-added suppliers likewise, as well as governments and user-industries as buyers. Government is increasingly a strong rule-setter, by imposing requirements for user-industries such as in the financial sector and critical infrastructures through ICT supply chain security in the NIS2 and DORA Directives. Likewise, governments are starting to set national requirements for public procurement of cloud.

In addition, there is substantial stimulus for cloud take-up by smaller user companies, notably in the Resilience and Recovery Fund (RRF) and substantial investment in R&D, while several EU countries have created favourable location conditions for data centres. All players are encouraged and stimulated by EU and GAIA-X cloud actions. There is a balanced approach to the development of the supply and demand sides from the perspective of competitiveness. The main remaining issues are lack of government engagement (as a major procurer) in some EU countries. Altogether, the right things seem to be done to have a vibrant industrial ecosystem, even if there is no overall plan at EU level comparable to the EU Chips Act.

Nevertheless, what about the 'hole' in the ecosystem? Will the company-agnostic approach result in strong EU players in basic cloud (e.g., OVH Cloud or edge cloud players that move into basic cloud or strong group of specialist basic cloud players (e.g., EscherCloud)? Or will this at best result in a set of strong value-added players in trust & security and in AI? EU cloud policy offers no answer to the

strategic issue of the hole in the ecosystem which risks inconsistency with EU company interests and EU geopolitical interests. See Figure 9. We return to this question below.

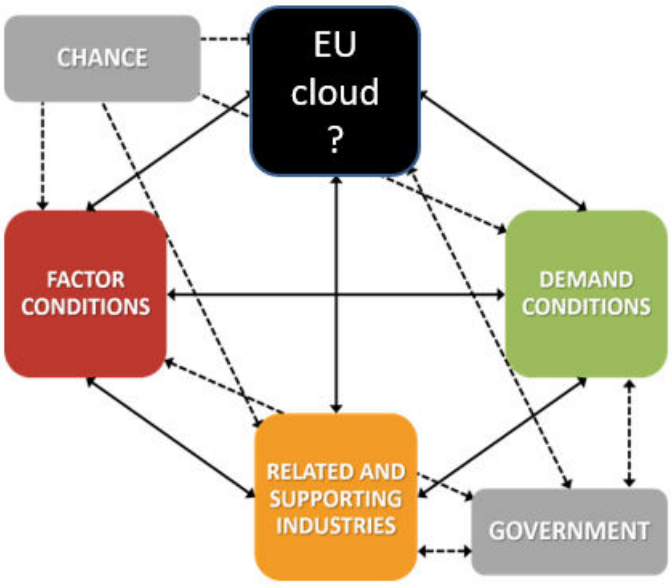


Figure 9: The EU cloud industrial ecosystem has a 'hole (modified from Figure 7)

International relations / geopolitics – geopolitical tension or strategic ambiguity?

EU user-companies may not care much about the home base of basic/generic cloud providers (and even not necessarily prefer US companies over Chinese), even though some recent market survey indicates a certain preference to buy European[75] and national sensitivity about Chinese but also about USA cloud providers has been growing. At this stage though, the USA pushes for harmonious and barrier-free trans-Atlantic cloud provision (such as expressed in the TTC) and there is no do-not-buy-China policy in the EU, let alone a do-not-buy-USA. Instead, collaboration is promoted (see above) and provider-neutral public procurement is the norm be it that some conditions are imposed regarding security, access to data, and data location (such as in France).

It is therefore also not yet clear what the answer from a geopolitical perspective is to the question what to do about the 'hole in the ecosystem', that is, the dominance of the main part of the cloud industry by US companies. Three ways forward were mentioned above:

- Build up strong domestic (EU) cloud providers.
- Accept the situation, compete on value-added such as AI/data analytics and trust services.
- Shift the paradigm away from centralised cloud.

Option 1 would risk creating conflict with the USA, not least in the TTC context and could spill-over to other areas where collaboration is desired by the EU, such as in semiconductors. Not tackling the problem of the hole in the ecosystem head-on is a form of strategic ambiguity that can be useful in

[75] (Toet, 2022).

the broader US-EU relationships. Nevertheless, from a competition perspective, a better-balanced cloud supply could be argued to increase consumer/user benefits. Ex-post intervention with competition policy has only limited effectiveness. Ex-ante intervention would be necessary too, through market regulation and public procurement. Contrary to the USA, an explicit Buy-EU or EU-First policy does not look feasible. However, national security interests can be a basis for selective public procurement. The envisaged Important Project of Common European Interest (IPCEI) on Next-Generation Cloud infrastructures and Services could boost EU cloud providers too. For now, however, a strong support for option 1 does not look likely and feasible and neither can we expect a sizeable shift to EU cloud providers thanks to public policy. Though they may have a superior offer and are gradually winning market share in their domestic markets, EU cloud providers are not yet winning at all[76].

Option 2 means accepting that foreign dependencies in cloud provision is here to stay. Accepting this must then become a key boundary condition for an explicit EU cloud industrial policy and that would then focus on value-added services. Such policy can be strengthened by integration with EU digital trust, data, and AI policies. Additionally, market-proscribing actions can be considered, such as strongly enforcing the mandatory and effective interoperability and portability of the DMA, making GAIA-X trust and interoperability specifications mandatory. Although this would be a significant departure in public communications about EU cloud policy, it largely is a continuity of *de facto* policy action so far.

However, choosing this option makes the EU cloud policy vulnerable to breakdowns in trust between the EU and USA which would in turn increase concerns about resilience, cybersecurity, and ultimately national security in the EU. It would therefore have to carefully be addressed in trans-Atlantic co-operation, notably in the TTC, being aware, however, that the EU may have little leverage for a balanced partnership as there is little reciprocity (there is little or no mutual interdependency). In trade negotiations, reciprocity may come from other domains too, but this likely complicates matters.

In addition, pre-emptive action will be needed to early-on deter anticompetitive behaviour of the big cloud platforms as that could wreck trans-Atlantic trust. One of the clearest but probably least feasible signals would be for the US to break up the large platforms and cloud companies. Option 2 leaves EU cloud providers out in the cold, accepting the already unequal playing field. It thereby causes a growing inconsistency with the current fairly company-agnostic approach.

Option 3 means changing the paradigm from central to distributed or edge cloud[77]. Edge cloud brings above all lower latency being closer to the user. In addition, it brings more user control and data localisation which are strategic autonomy benefits. Potential but still to be demonstrated downsides can be reduced economies of scale and security (the latter, as the cybersecurity attack surface increases).

[76] (KPMG France, 2021).
[77] Or cloud-edge as it is called in (Vodafone, 2022).

A strategic approach to edge cloud is currently only partially developed even though the concept was put forward with much visibility by the European Commission. It still needs to be further substantiated (by means of an impact assessment) and be supported by targeted policy. The European Commission also suggests considering synergies with the semiconductor policy (chips for edge computing) and manufacturing (Industry 4.0). Likewise, synergies can be sought with 5G/6G policy - possibly including OpenRAN. The European Commission should then come forward with such an edge cloud industrial policy.

Time is of the essence, though. Foreign cloud providers are already gearing up for edge cloud too and rolling out related physical assets such as server centres and in particular in the telecoms market they already get a strong position[78].. If the EU waits long coming forward with a clear edge cloud industrial policy the result will be another hole in the ecosystem.

As in other areas for digital industrial policy, the EU's challenge is to meet several policy objectives: strategic autonomy in cloud (loosely called 'cloud sovereignty'), competitiveness of both a sustainable EU cloud industry and cloud user industries in the EU, and societal benefits from cloud efficiency and innovation. In policy terms this means that an edge cloud industrial policy must address regulation and other measures for trust and security of access to, use of and location of data; the international dimension of EU requirements including in trade policy and FDI scrutiny; user-provider ecosystem facilitation such as (public) procurement standards and guidance as well as pilots as well as regulation to address competitive conditions; IP control; and research and innovation of EU firms notably where technology can alleviate sovereignty concerns about access to sensitive data (such as homomorphic encryption). One could argue that most such policies are present (e.g., Data Act, DMA, GAIA-X, cloud certification, EU R&D funding) but this is still far from a coherent edge cloud industrial policy, let alone that it is clear how these policies would deliver on those objectives mentioned above.

It has been assessed[79] that cloud adoption and value creation from industrial data exchange could be significantly larger than any other approach if the cloud market stays open for foreign providers combined with strong EU-wide, harmonised trusted cloud regulation and free flow of data across approved jurisdiction. However, the yardsticks for EU cloud industrial policy are concern both economics and sovereignty. It is not clear how the dynamics in the market will develop, given the strong position of US cloud companies and their deep pockets, and therefore to what extent such an approach would address geopolitical concerns (i.e., the issues will be whether critical cloud providers are under foreign control and whether there is then adequacy in compliance with EU regulations that can stand the test of the European Court of Justice, cf., the Schrems court cases).

EU policy aiming to ensure strong EU presence in edge computing is also likely to generate geopolitical clashes. Firstly, with the USA given its cloud hegemony,. Secondly, given the EU's objective to keep

[78] See e.g., (Stocker et al., 2021).

[79] (Vodafone, 2022) presents three scenarios. The 'globalised free market' scenario is closest to option 2 above, 'fortress Europe' is closest to option 1, whereas the third scenario has aspects of option 3, though the options in the present report put larger emphasis on the geopolitical aspects and to some extent on the potential of technology.

control of its industrial, transport and logistics data, also with Japan and Korea who will defend the interests of their large export-oriented manufacturing industries.

EU policymakers have to reflect on control and capacity of standard cloud provision in Europe, considering the geopolitical and economic consequence of various options (a comprehensive strong EU cloud ecosystem, a cloud value-added services ecosystem, an edge cloud ecosystem). The analysis is summarised in Table 2.

Table 2: Gaps and inconsistencies in EU cloud policy

Risks	Gap or inconsistency	Proposed policy action
Lack of coherence of cloud initiatives, at national and EU level, creates confusion and uncertainty in the market	Single, integrated, and coherent EU cloud policy does not yet exist, even if there are many cloud actions	Provide single EU Cloud policy (taking into account recommendations for edge cloud)
Inconsistency between EU cloud company interests, influence on cloud industrial ecosystem in the EU, and EU geopolitical interests	EU cloud policy offers no answer to the strategic issue of the hole in the ecosystem	EU policymakers to reflect on control and capacity of standard cloud provision in Europe, considering the geopolitical and economic consequences of the three options
Lack of coherent edge cloud policy risks the repeating of the erosion of EU strategic autonomy, competitiveness, and innovation of the current centralised cloud ecosystem.	Policy elements are present but have not been brought together and analysed in terms of impact in industrial policy at the three levels of the analysis in this report	EU to develop a coherent edge cloud policy analysis on: • trust and security regulation (data portability, unbundling or decoupling of cloud, and added value and trust services), • competitive conditions (cloud switching), • demand-supply facilitation (public procurement guidance), • trade policy (adequacy conditions, FDI constraints) • internationalisation (edge cloud standardisation) • IP (protection) • R&I (cloud technology for sovereignty-by-design) • Edge cloud metrics (EU market share, adoption, economic value, innovation, EU strategic autonomy).

Persistent strategic ambiguity as regards cloud in the EU creates market hesitation for cloud adoption and underuse of potential of industrial data.	No choice made between the three options or a combination of them.	Following the edge cloud analysis a weighted choice is to be made on one option or a combination of them.
Underused potential of wider EU digital policy, weakening impact of EU cloud policy	Lack of comprehensive view spanning several specific digital policies	EU cloud policy must consider the linking up with related semiconductor, digital identity, or cybersecurity policies

4.3. Digital Identity

4.3.1 General

Digital identity is a portmanteau for electronic identification, electronic signatures, other authentication services and the emerging digital wallet services. All of these are related in what are called trust architectures. Electronic identity is widely used, mostly coming from private non-EU providers (e.g., social media ID or email address, usually with relatively weak security) with in second place eID provided by governments, mostly with strong security. There are, however, large variations across Europe. Estonia has a single government-run digital ID system, in Belgium a private-public co-operation provides a wide range of public and private services based on a single national eID, whereas Germany is still in the process of rolling out government-issued eID. All countries, however, have identification of citizens. Recognising such identification is a sovereign function, a *fonction régalienne*. Citizenship is a sovereign asset.

4.3.2 Analysis of situation

Company level – strong concentration, ever-expanding foreign large cloud/platforms

As is the case for cloud, in the digital identity / digital wallet world the distinction can be made between basic providers of the digital ID/wallet infrastructure, the value-added providers and system integrators such as for data analytics or integrators into application areas like banking, and the professional buyers such as banks and governments. In addition, and more than for cloud, the end-user, the citizen, is an actor.

In its simplest form, digital identity is just a piece of data and some security software such as a username and an encrypted password which is handled by secure software for authentication. Infrastructure companies implement digital identity in hardware (smart card chip, mobile phone with a SIM card, secure devices). They do so in order to harden security. The traditional hardware SIM is threatened by soft-SIM and virtualisation, i.e., a digital identity in software while the secure hardware is a generic function of the phone or computer. Blockchain and other technologies enable decentralised and distributed eID/Wallet systems. This is called self-sovereign identity (SSI) if control off the user data remains in the hands of the citizens. Platform companies (Meta, Google, Microsoft, Apple) have expanded into digital identity including digital wallets. This can give them a firm lock on the user as they can combine the digital identity with user transaction and interaction data. Given the convenience and ubiquity of those private eIDs there is already strong citizen capture, posing a

challenge to government's sovereign role. Likewise, there is strong consumer capture which is a challenge to smaller private or not-for-profit digital identity suppliers, as well as to providers of a wide range of public and private services which very often require a form of digital identification. The response of EU policy is discussed below.

National competitiveness/industrial ecosystem level – an incomplete ecosystem

In the EU, several components of an industrial ecosystem are in place such as eID suppliers, government as buyer, government as regulator, and government as financer of public eID infrastructure. The large presence of foreign platform companies is disrupting the EU harmony: the operators of digital identity consist of a few dominant non-EU platform providers and the EU governments. The latter can mandate private operators such as banks to act as digital identity providers as happens in Sweden (European Commission, 2019). They also provide digital wallets which are still in limited form today (e.g., containing a COVID pass) but should take off soon. Taking these suppliers as the central point in the ecosystem analysis, related industries include mostly European large identity and authentication hardware/software suppliers such as Thales and larger and smaller system integrators such as Guardpoint.

An important related industry is also the secure hardware industry, which can be part of the earlier-mentioned suppliers but also pure hardware security module companies such as Utimaco. In future, value-added services to the digital wallet may develop such as user data recording and AI-based interaction and behaviour analytics (conceptually the wallet is a representation of the user and her/his interactions in the digital world).

At the demand-side, governments worldwide are large buyers, and many sectors continue in their digital transformation which will generate more and more demand for digital ids/wallets. Given the sovereign dimension of digital identity, many countries worldwide have already or will further regulate the market in order to protect citizens, create legal certainty, and ensure cyber-resilience.

International relations/geopolitics – the geo-politisation of digital identity

Digital identity has not been drawn yet into geopolitical rivalry between states, but as explained, the strong digital platforms and cloud providers have been treading into sovereign space with their grip on citizens identification. As these platforms are foreign-controlled, states get concerned and thereby digital identity does become geopolitical. In addition, citizens, as a major actor in the ecosystem have become increasingly wary about surveillance for commercial interests by companies. Likewise, they are concerned about state surveillance. They have read about mass-suppression by monitoring individuals in China and Russia. They got sensitised about tracking of individuals in the interest of public health during the COVID-19 pandemic or in the interest of public security in the combat against terrorism. Therefore, any digital identity solution is in the spotlight, gets easily politicised and can get drawn into geopolitical ideological battles. At the same time, governments are also not sure whether blockchain-based self-sovereign digital identity could undermine their centralised approach to sovereignty. Governments are treading carefully, domestic, and international.

4.3.3 Analysis of EU digital identity policy

Here we summarise the most salient elements of EU digital identity policy, analysing this at the three levels and interlinkages between these levels[80].

The cornerstone of EU policy is the eIDAS Regulation, which will be succeeded by the European Digital Identity Regulation. The legislation is focused on legal recognition of eID, eSignatures, and mutual recognition across the EU, in order to ensure the functioning of the internal market. The new Regulation also introduces legal recognition for and roll-out of digital wallet solutions. EU legislation is strongly based on legal and technical interoperability of national eIDs (even the European Wallet is linked to national eID). The legislation is also linked to financial sector legislation notably Anti Money Laundering (for Know Your Customer or KYC). Furthermore, the EU provides R&D and piloting support, for instance of Large-Scale Pilots on the digital wallet[81], and substantial digital infrastructure deployment support through the Connecting Europe Facility (CEF), Digital Europe programmes, and the Resilience and Recovery Fund (RRF). Finally, there is an important link between the proposed European Digital Identity Regulation and the Digital Markets Act as explained in the next paragraph.

Company level – neutral except as regards very large platform providers

There is no EU policy that is specific to certain companies in digital identity, except that platform regulation (DMA) breaks the proprietary coupling of platform and digital identity of the very large platform companies, while the European Digital Identity Regulation enforces that national eIDs cannot be refused. Nevertheless, even if there is such decoupling, platform providers can continue to run both their identity scheme and the platform, i.e., there is no full functional separation or breaking up of these platforms. The combined legislation of DMA and digital identity is therefore not neutral as regards the providers. There is no policy to stimulate emerging companies or alternative providers and no link from DMA to other policy measures (such as funding) that are specific to the type of companies that can fill the opening created by decoupling.

National competitiveness/industrial ecosystem level – incomplete and not yet thriving

DMA and the EU Digital Identity Regulation together should stimulate competition between providers and EU providers should be able to benefit, but it must still be assessed whether EU providers actually benefit from digital identity and platform regulation. As regards the factor condition of expertise and knowledge, the EU has a strong position, which is maintained by EU R&D funding. Demand-side interest and government-as-buyer is promoted by the legislation and by EU funding programmes but here too there is a missing connection to stimulate the digital wallet demand and take-up in a wide range of use cases. The EU risks repeating the slow take-up, compared to the speed of adoption achieved by the large platforms, of the previous phase of digital identity.

[80] A more extensive description is in Annex II.
[81] For Large Scale Wallet Pilots, see: https://hadea.ec.europa.eu/events/webinar-large-scale-wallet-pilots-call-explained-2022-04-06_en

International relations / geopolitics – rapid rise of foreign influence is a distinct possibility

EU policy does not address ex-ante the risks of M&A and foreign investment. The stopgap can be the EU FDI Regulation. EU policy needs to put in place a digital identity market watch, in particular as regards foreign actors and capital as well as related emerging areas such as AI. Ex-ante protective measures may not be necessary as several EU players from related industries are also large. EU policy includes active international outreach in digital signatures standardisation and blockchain development. The positive international experiences with the COVID pass where over 60 countries with more than 1 billion citizens have joined the EU system[82], provide a solid basis for international adoption of the EU approach to digital wallets. The international potential of EU digital identity is promising but policy is underspecified.

In digital identity there is no articulated EU digital industrial policy at the moment. Yet, it is an area of important economic value added. Moreover, there is a strong basis of regulation and industrial activity in Europe, which enables to develop such an industrial policy. It is an area of huge strategic autonomy importance where powerful private sector players such as platform companies can take control of economic competitiveness and aspects of sovereignty.

The analysis is summarised in Table 3, ordered by priority.

Table 3: Gaps and inconsistencies in EU digital identity policy

Risks	Gap or inconsistency	Proposed policy action
Repetition of past failures such as low take-up, loss of value in EU, erosion of sovereignty	No articulated EU digital identity industrial policy	Put forward (urgently) a comprehensive EU digital industrial policy for digital identity/wallets
Underspecified policy despite the promising international potential of EU digital identity	Lack of international dimension on digital identity strategy, and lack of attention to digital identity in EU international strategy	Develop an international digital identity policy for the EU
Promising developments by companies in the EU are appropriated by foreign actors, leading to loss of sovereignty	No attention for foreign investments	Put in place a digital identity market watch, in particular regarding foreign actors and capital as well as related emerging areas such as AI

[82] (European Commission, 2021c).

5. INSIGHTS FROM THE SELECTED CASES

The three cases presented above give insights into the methodology of analysis and a number of cross-cutting themes.

5.1. Methodological

This study offers a framework for to analyse and construct industrial policy which must meet competitiveness and strategic autonomy purposes and respond to company needs.

Case analyses are useful in an abductive approach[83], meaning that we start the analysis with an initial framing (or 'enframing'[84]) in order to then identify relevant patterns and generalise from them. Our initial frame of mind is captured by Figure 5 'Three perspective on digital industrial policy'. We also aim for consistency, completeness, and impact of policy.

From the case analyses, the approach is quite revealing as regards consistency and completeness. It provides less insight, however, in the impact of policy. Nevertheless, the approach raises warning signals about missing elements that likely make the specific policy less impactful or even counterproductive.

At the same time, we can easily go down the rabbit hole, as the analysis requires and produces a large amount of information. This is hard to process for policymakers. To still communicate effectively about the analysis, we can present the most relevant elements in a narrative, applying the Narrative Policy Framework, NPF (Jones & McBeth, 2010). Ideally, the analysis is presented as a short narrative of a few pages. Narratives are an important tool to communicate (digital industrial policy) thinking to experts, policymakers, CEOs and politicians and provide for a setting, actors, plot, and solution.

5.2. Institutional Capability and Capacity

All cases show that there is a significant challenge in policy development. Having to combine three perspectives and take into account the characteristics of 'digital' makes for a very complex exercise. Nevertheless, this is what such policymaking is about and what the EU has to expect that geopolitical partners, competitors and rivals do too. Integrated policy must be the aspiration. China's industrial policy in several respects shows the way to connect domestic investment with international policy such as the Belt and Road initiative, to connect planning for its universities as in China 2025 with international standardisation such as in the ITU, to relate public procurement with market access requirements, etc. Institutional capability and capacity are part of geopolitical rivalry and competition.

An additional complication is the interplay between government and business and technology developments, or governmentalism[85]. The mutual conditioning of technology and social constructs such as policy or strategic autonomy / sovereignty is also expressed as 'code is law' and 'law is code'[86].

[83] (Friedrichs & Kratochwil, 2009).
[84] (Heidegger, 1977).
[85] (J. E. Cohen, 2019).
[86] (Lessig, Lawrence, 1999; Timmers, 2022a).

Finally, policymaking is only step one. The second step is policy implementation, which requires different capabilities and also significant resources. As mentioned before, EU Member States are increasingly willing to have digital and industrial matters dealt with at EU level and align national policies to what comes from the EU. Moreover, in recent political decision-making on DMA and DSA, as well as on 5G security, increased implementation powers have been given to the European Commission or agencies such as ENISA. All of this can be argued to strengthen EU strategic autonomy, at least in intent.

In the case of digital industrial policy, the same holds, at least for the three cases we analysed. The European Commission or other authorities must, however, still build up implementation expertise (capability) and be given resources (capacity). Not doing so amounts to emasculating strategic autonomy right from the beginning.

Integrated policy that is complete, consistent, and coherent, is an aspiration but hard to execute. Some room for comfort can be that, in geo-political and geo-economic perspective, EU integrated policy is about relative advantage to others. The yardstick should therefore be to compare to the best (i.c., China). Building experience with integrated policy must come with a sense of realism. This could develop by focusing on limited areas. Examples are edge cloud, digital identity, or hardware security (Hardware Security Modules, HSM).

5.3. Policy Completeness

A theme that emerges from all cases is that policy as proposed is incomplete. Partially, this is caused by silo-thinking, where policymakers limit themselves to their area of responsibility. Notably, we see missing elements in mobilising foreign/international policy to digital matters, even if there is recognition that EU digital industrial policy has international aspects too; and in complementing regulation with financial instruments such as shareholding or risk capital.

Yet another aspect of completeness emerges from the cases, namely that the digital industrial policy of each case should be related to the other cases. Semiconductors are related to edge cloud, digital identity is related to cloud and semiconductor security. This is a pattern that is more general. We already mentioned cybersecurity as being related to most digital technologies. AI is a digital technology that manifests itself in several layers of the stack diagram (Figure 2 Technology stack view of digital industry). This provides us one important element of the overall strategy for digital industrial policy, namely, to positively and pro-actively build specific digital industrial policies so that they complement and reinforce each other.

5.4. Policy Consistency

Another theme that emerges from all the cases is the fact that there are noticeable inconsistencies, notably between objectives at company level, at ecosystem level, and at international level. Partly, this is due to incompleteness, for instance, ecosystem policy action that is not complemented by international action. Partly, it is due to a lack of clear choices, creating ambiguity. And, partially, it is due to a lack of insight into how actions at one level relate to actions at another level.

A second, less explicitly visible inconsistency is about the discrepancy between a strong policy and a

weak implementation. This is illustrated by past experiences in digital identity, cloud, and semiconductors. Partly, this is due to a gap between strategic intent and strategic planning. The European Commission, for instance, acknowledges with candour that past semiconductor initiatives were largely unsuccessful due to a lack of political commitment and the industry's short-term orientation. Partly, however, it may also be due to a lack of institutional capacity.

5.5. Digital Industrial Policy as Integrated Policy

A conclusion then is that EU digital industrial policy must be an 'integrated policy', meaning coherent, consistent, and complete. With that in mind, it will be necessary to:

1. Mobilise EU internal policies and external policies: internal market, EU R&D, Art. 173 industrial policy, competition policy as well as trade, foreign policy, and international regulatory and investment co-operation
2. Make sure internal and external policy interventions are coherent, consistent, and complete
3. Strive to make digital industrial policy in one specific domain complement and reinforce digital industrial policy in in other domains.

5.6. Risks and Pitfalls

The analysis points to several risks in developing and implementing (digital) industrial policy in the EU. At a general level this includes an exaggerated belief in planning and 'plan-ability'. It also includes the risk of repeating past mistakes. In the digital area this includes not taking the winds of change seriously or not even being aware of them or being too self-confident (the Minitel case springs to mind). It also includes the belief that history repeats itself, i.e., denying that the digital and geo-politicised and globalised world of today is qualitatively different from the past.

More generally, while the Washington Consensus was clearly in the interest to global capitalism – the large tech companies included - it also brought the benefits of enhanced productivity to many (Lewis, 2005). Abandoning this and swinging over to regionalism and fragmentation will make it much more difficult to tackle global challenges such as climate change and peace and risks igniting populism and social unrest. EU digital industrial policy needs to lead the way in a balanced approach to both geopolitical and global challenges.

At a more specific level we must recognise risks in relation to the EU. The red thread of this report is that international and geopolitical developments may overtake well-intended EU intentions. Moreover, the EU has a limited mandate in industrial policy: Article 173 of the Treaty on the Functioning of the European Union (TFEU) allows for coordination, guidelines, exchange of best practice, monitoring and evaluation, and moreover, explicitly excludes regulatory harmonisation. This suggests that firm industrial policy is basically a matter of each Member State.

On the one hand this is correct. The EU institutions have to tread carefully to not overstep their mandate in proposing industrial policy. More than once we see that especially Germany or France takes the lead in industrial policy initiatives that subsequently are 'Europeanised' (a case in point would be an EU cloud industrial policy). Moreover, Member States are free to develop

intergovernmental industrial policy and can even make use of Treaty-based industrial policy action, namely IPCEIs[87],[88].

On the other hand, this is not correct. Firstly, the EU has quite skilfully made use of other legal bases to underpin industrial policy. For instance, the EU Chips Act also uses the internal market legal basis Art. 114 TFEU which is a very strong basis for regulatory harmonisation as well as the research & technological development legal basis, Articles 182 and 183 TFEU, which have been shown to enable jointly building R&D capabilities and capacities. Secondly, EU Member States increasingly recognise that the only geopolitically sensible industrial policy for themselves is a joined-up policy at EU level. This even holds for the largest actors, Germany and France, who recognise this explicitly. Thirdly, recent EU policymaking shows some remarkable changes: it is much faster than in the past (the DMA and DSA were adopted in just over a year whereas often 2-3 years are needed; COVID recovery financing was decided in a matter of months; the first wave of sanctions against Russia were a matter of weeks).

There is also a greater willingness amongst EU Member States to handle certain matters at EU level, in particular in the digital domain, all being well aware that 'digital' transcends the control they may have within their borders. Even more, Member States are willing to accept EU action in matters of limited or restricted mandate at EU level, such as health, sharing of state debts (in the RRF/NextGenerationEU), defence (Ukraine), and even in national security (5G security). Fourthly, and remarkably, in certain matters Member States accept or even propose more implementing powers at EU level, notably for the European Commission (such as setting up an implementing capacity for DMA and DSA, (Breton, 2022a)). Conversely, the European Commission has been able to operationalise forms of shared industrial policy between coalitions of the willing in the mechanism of Important Project of Common Interest (IPCEI) that is starting to get significant traction[89]. It is too early to say whether the European Commission is, next to policymaker also becoming an implementing authority in digital industrial policy. This does not look likely for now. Nevertheless, a public discourse is necessary for democratic accountability on digital industrial policy 'orchestration'.

Nevertheless, lingering risks in EU governance remain: sustainability of reinvigorated decision-making, keeping up political interest, *juste retour* tensions (IPCEIs rarely involve every country and industrial ecosystems policy tends promoting clusters in most advanced economies), lack of governance capacity and capability, and the limited mandate of the Treaties that may prevent a truly coherent industrial policy as is a must in geopolitical competition.

The table below captures risks, while the suggested remedies relate to the recommendations in the next chapter.

[87] Art 107 TFEU and (Communication from the Commission Criteria for the Analysis of the Compatibility with the Internal Market of State Aid to Promote the Execution of Important Projects of Common European Interest 2021/C 528/02, 2021).
[88] For IPCEIs Member States do not need to invoke Art. 20 of the Treaty on the European Union (TEU) on Enhanced Cooperation.
[89] For IPCEIs in semiconductors and edge cloud see resp. section 4.1 and section 4.2.

Table 4: Risks for digital industrial policy development

Risks	Risk level	Remedies
Geopolitics and international economics	High	EU digital industrial policy needs to be closely integrated with EU foreign policy
Waning political interest, eroding EU decisiveness	High	Connect to core concerns on strategic autonomy such as security, defence, democracy
Limited mandate in EU treaties	Medium/Low	Combine soft with hard legal bases, advance the debate on renewal of competition policy
EU governance capability and capacity	High	Launch a debate on digital industrial policy governance, linking to hard commitments
Juste retour requirements in political negotiations	Medium	Continue stressing that sovereignty concerns measures in all of economy, society, and democracy
Erosion of democratic accountability	Low/Medium	Public discourse on the need for and cost of EU digital industrial policy, changes in decision-making, and Europeanisation of implementation powers
Confusing the future for the past	High	Pro-active monitoring required to move forward into flexible and anticipatory policy- and rule-making

6. POLICY RECOMMENDATIONS

6.1. Industrial Strategy and Geopolitics

This report stresses the importance of geopolitics as a driving factor for industrial policy, which expresses itself in the need to pursue strategic autonomy in order to safeguard sovereignty. One might call it a 'geopolitical digital industrial strategy'. For strategic framing of specific industrial policies, we recommend for the EU to:

- Combine three perspectives: EU strategic autonomy, national/EU competitiveness, and business/firms performance;
- Take into account in developing digital industrial policies that 'digital is different', in terms of speed, scale, systemic nature and the power of synchrony;
- Ensure completeness, consistency and impact of specific digital industrial policies within the combination of these three perspectives.

Over the past decades industrial strategy was relatively loosely coupled to geopolitics. This report argues that a strong coupling is necessary given the reshaping of the world of industry by geopolitics, global challenges, and digital technology developments.

An example would be to address ex-ante – because of its geopolitical impact - the international dimension of state aids and other government support and, moreover, as challenging as it will be, to seek to do so in dialogue with like-minded partners.

6.2. Digital Industrial Policy Development

6.2.1 Completeness

All cases clearly show that digital industrial policy must consider all policy instruments, from any relevant policy domain. That is, a specific digital industrial policy may address market failures and strategic autonomy with investment, market regulation, standardisation, private-public and private-private collaboration, international trade measures, in complement to competition action, international outreach, etc. It should be expected that policymakers explain and justify why certain instruments have not been mobilised. In the cases, we notably observe weaknesses in including foreign policy action.

6.2.2 Consistency

The cases clearly show that consistency of policy actions is a challenge, in terms of relating the international system of states, industrial ecosystem, and firm levels. This is not only a missed opportunity but also a high-risk gap in international comparison with China. Notably weakly connected is strategic autonomy as a driver.

6.2.3 Impact

Though specific industrial policies have deliverables, these tend to be formulated in absolute terms rather than relative to the relevant geopolitical or international-competitive situation. Moreover, they do not tend to foresee flexibility to adjust to technological and geopolitical developments.

All three aspects point towards putting in place **strong, pro-active monitoring which must be closely connected to flexible policy adjustment**, that is a process to adjust a specific digital industrial policy to maintain completeness and consistency and to ensure relevant impact. This is an **urgent matter**, which should start now from a dependency / chokepoint analysis.

Moreover, gaps in existing digital industrial policies need to be addressed as a matter of urgency. For the three cases, see below.

6.3. Priorities for Digital Industrial Policy

We can envisage three approaches to prioritise digital industrial policy:

1. We can use the **technology stack** diagram and take topics from each level and/or cross-cutting topics such as cybersecurity. The choice could be fine-tuned to also consider dynamic competition benefits, i.e., the extent to which such as technology enables or stimulates innovation and investment in general[90]. A special cross-cutting topic is open-source software for which the USA Senate Homeland Security Committee proposed a bill[91].
2. Policy analysts identify important **technology trends** e.g., (McKinsey, 2022) lists applied AI, metaverse, Web3, applied AI, industrialised machine learning, cloud/edge computing, digital identity, 5G/6G, quantum technologies, and next-gen software development.
3. Yet another approach would be to ensure that digital industrial policy addresses **key user industries and the core of government** in Europe[92]. Relevant key user industries in the EU include automotive, telecoms, and health/pharma. These certainly need specific semiconductors, security, applied AI, 5G/6G, edge and centralised cloud, IoT, industrial/corporate platforms and dataspaces, as well as digital ID and in the somewhat longer term, quantum technologies. This approach would thereby both address these key technologies and these key users.

We advise to now pursue the **key user industries and the core of government** approach in order to address the gaps such as in applied AI, dataspaces, and sectoral platforms; and to **complement this with a thorough reflection on the technology stack**. The latter is beyond the scope of this study.

6.4. Policy Responding to the Nature of 'Digital'

The speed, scale, systemic impact, and power of synchrony that characterises the digital world risks leaving policy development as we know it behind, rendering it increasingly irrelevant or even misplaced. **Pro-active monitoring, mandated experimentation with legislative flexibility, and responsiveness** by mobilising the whole toolbox of policy instruments must be investigated. This is to some extent recognised. At EU-level, the recently proposed AI Act allows for a degree of experimentation though legally mandated sandboxing. The Joint Research Centre is actively contributing to forecast studies, and so is the case for many European projects. But this is not effective

[90] (Carretero, 2022).
[91] (Matishak, 2022; Peters, 2022).
[92] This would also more closely fit with the approach of some companies, for instance, Apple has set out to do so (Hofer & Scheuer, 2022).

enough. The EU, with its regulatory power and 'Brussels Effect', should lead the way in the renewal of policymaking.

6.5. Specific Digital Industrial Policies

This section gives the main recommendations for semiconductors, cloud, and digital identity.

6.5.1 Semiconductors

The greatest challenge for EU semiconductor industrial policy is to complement the current EU Chips Act with a fully geopolitical approach, that **addresses geopolitical developments, including the risk of conflict such as subsidy races with 'like-minded' partners**. In doing so the EU can build on existing and emerging international co-operation, notably with the USA in the trans-Atlantic Trade and Technology Council and develop a rolling impact assessment on investments and funding. Full recommendations are in Table 1: Gaps and inconsistencies in EU semiconductor policy'.

6.5.2 Cloud

The analysis points to **the relatively weak position of the EU in basic/generic cloud provision**, a position in the industrial ecosystem that is occupied by foreign (US) providers. A strategy must be developed to deal with this 'hole' in the EU cloud industrial ecosystem. An assessment is needed of a potential shift in paradigm to edge cloud. If the outcome is that this is either of limited relevance, or that EU providers will not be able to become major players, the EU will have to accept a long-lasting foreign dependency and thus lasting risks to its strategic autonomy. A risk management approach must then be developed. Full recommendations are in Table 2: Gaps and inconsistencies in EU cloud policy'.

6.5.3 Digital identity

The main recommendation is to now **propose a real EU digital identity industrial policy**. Several policy elements are present at EU level but the lack of an explicitly formulated policy, and the lack of connection between the various policy elements makes the EU highly vulnerable for the loss of autonomy in a core aspect of sovereignty, citizen identity. Full recommendations are in Table 3: Gaps and inconsistencies in EU digital identity policy'.

6.6. Institutional Capacity and Capability

Digital industrial policy requires **new institutional capabilities** with adequate resources (capacities) for complete, consistent and flexible industrial strategy development and related specific policymaking. It is quite daunting to understand the challenges from the geopolitical to the ecosystem and down to the firm level. Let alone, to combine policies from areas as diverse as trade, R&D, standardisation, investment, and foreign affairs… Nevertheless, there is no choice but to take up the gauntlet. The EU's future, economically, socially, and politically, is at stake given that China as a geopolitical rival thrives on our institutional weaknesses.

Special attention is needed for policy implementation. Above all matters to 'execute, execute, execute!'. For **democratic accountability** it is important to discuss if and how implementation

(execution) should be anchored in European Commission, in Member States' authorities or in separate bodies. In the meantime, elements are arising EC-internal[93], in Joint Undertakings and in IPCEIs.

In the digital field given scale, speed, synergies, and synchrony of 'digital' the only realistic way to pursue industrial policy is jointly at European level. This does not exclude at all that there are national DIPs but does require that these align with and create synergy at EU level. Given the lack of Treaties mandate to go beyond coordination of national industrial policies, such Member States-EU alignment in **digital industrial policy must be strongly supported by European Council political agreement**. Making resources available at the EU institutions and for the Member States would greatly facilitate this approach.

Next to the governmental institutions, institutional capacity building is also a must in European Standardisation Organisations and in industry organisations. It is in the same spirit of enabling much more complete, coherent, and flexible digital industrial policy, that builds on a profound understanding of motivations of firms, competitiveness and innovation in industrial ecosystems and the actual geopolitics of the system of states in the digital age.

[93] (Breton, 2022a).

7. CONCLUSIONS AND NEXT STEPS TOWARDS AN EU DIGITAL INDUSTRIAL POLICY WORKPLAN

This report suggests an original approach for an EU digital industrial policy (DIP) adapted to a time of rising geopolitical tensions, global challenges, and disruptive digital technology developments. It provides a set of concrete recommendations that can be and should be applied to EU DIP. It explains how to avoid pitfalls and risks. Finally, it presents concrete recommendations for the three selected case studies. The gist of these is to **urgently address the geopolitical dimension of the semiconductors economy, to develop an edge-cloud strategy, and to put in place a full digital identity industrial policy**.

The report also identifies the need for further analysis. This should address specific DIP areas and governance patterns to strengthen the internal legitimacy of EU DIP-focused action and to move towards EU digital industrial strategic autonomy in its full breadth and depth.

More specifically, building on the reflection on prioritisation in section 6.3, the suggested additional high-priority areas for which the contents of a concrete EU digital industrial policy should be identified are as follows:

1. **Quantum technologies, 6G**: to ensure EU presence in highly strategic fast developing areas for industry where the EU can still act in the frontline rather than having to catch up;
2. **Hardware and software security (IoT included) and smart cyber-defence**: to protect and defend the core of government, where full EU autonomy may be required in certain aspects;
3. **AI, open source**: these two cross-cutting, competitive topics are of huge industrial and geopolitical relevance , as the EU must boost its industrial position and claim a strong role in the international agenda-setting on norms and standards;
4. **Assessment** of coherence, completeness and impact of EU digital industrial policy **from the perspective of major EU user industries** including automotive, manufacturing (industry 4.0), health and pharma, finance, as well as defence and government.

ANNEX I: ADDITIONAL THEORETICAL BACKGROUND

Three perspectives are used in this report. Each of them has to some degree a take on industrial policy. In academic literature one can find only limited linkages between the three perspectives. Below we provide some theoretical background on each of the three perspectives and on notions that link the three perspectives. Before doing so, let's provide a brief description of the types of industrial policy interventions.

Industrial policy interventions

Industrial policy deals with the industrial ecosystem. We can represent it as in the diagram, drawing attention to the actors (especially firms and the state). Their interplay gives rise to objects such as markets, value chains, and value networks. The industrial ecosystem produces specific products and services, therefore we say e.g., the cloud industrial ecosystem. The demarcation line between what is inside and what is outside is an important choice – and we may get it wrong especially in the fast-moving digital domain.

Industrial ecosystem policy interventions target the objects of the ecosystem such as market and value networks and the objects within these such as prices, standards, partnerships etc. Industrial policy must first of all define what the industrial ecosystem is (cloud, semiconductors, etc). Then, the traditional actions concern facilitating, modifying, substituting, and proscribing (parts of) the industrial ecosystem. Where the object is the market, these are illustrated in the box below[94].

Further actions can be added to this, such as transitioning from an existing industrial ecosystem to a new one. This may be useful to consider when there is an industrial paradigm change such as the transition from fossil fuel to electric in the car industry, or possibly for a transition from centralised cloud to edge cloud. Logically, one can also imagine policy action to terminate an industrial ecosystem (not relevant for our cases). Industrial policy has a national or regional (EU) scope. Therefore, likely also external or foreign / international relations policy actions are part of the industrial policy, e.g., in trade or international standardisation. Identifying these external actions is a necessity, given that in this era – as argued throughout this study – geopolitics is a major determinant of industrial policy.

[94] See (Aggarwal & Reddie, 2018) and for an application to EU cybersecurity industrial policy see (Timmers, 2018).

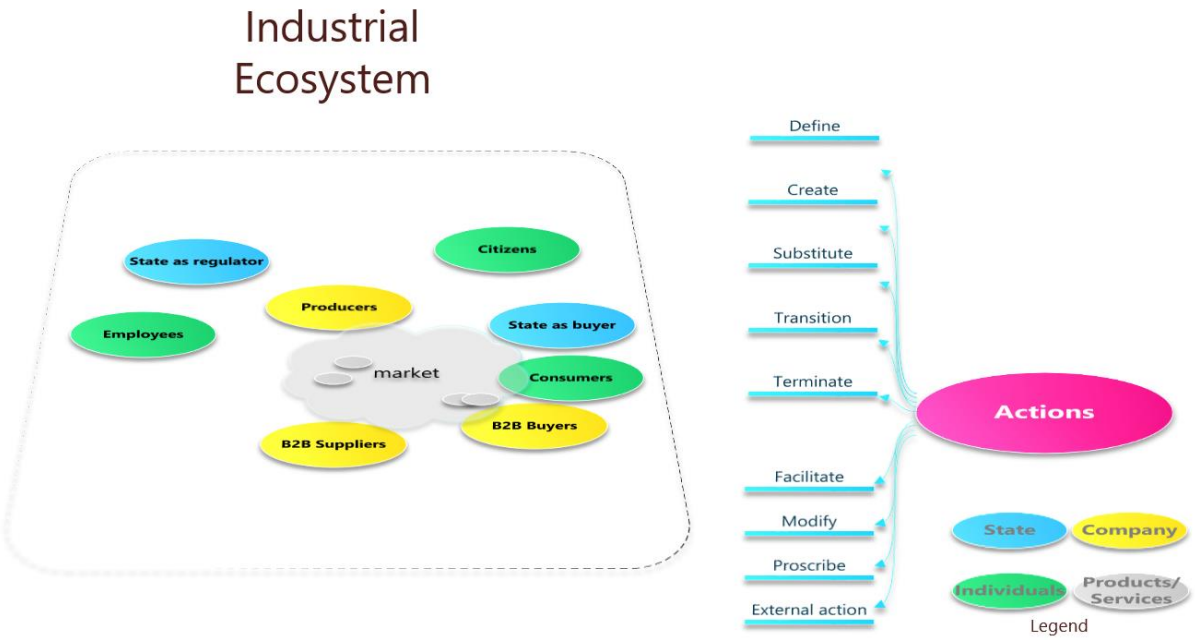


Figure 10: The industrial ecosystem and policy actions

Market Creating involves public policies designed to create markets, by establishing rights, incentives and opportunities for exchange; e.g., creating a market for air pollution "rights."
Market Facilitating involves policies that promote or improve the operation of markets by reducing transactions costs, enhancing incentives, or internalizing benefits and costs; e.g., public investment in transportation to expand the geographic scope of markets by reducing transport costs.
Market Modifying involves the creation of regulations that attempt to change the conduct of subjects, the objects, medium or terms of exchange, in order to produce outcomes different from those the market would otherwise produce; e.g., agricultural marketing orders.
Market Substituting involves policies that create substitutes for markets, in which instruments of political authority are used to allocate or distribute resources or control conduct of individuals or organization's outcomes are achieved.
Market Proscribing involves policies that attempt to prohibit exchanges by particular subjects or of particular objects, with no attempt to use authority as a substitute method for achieving a given outcome; rather, authority is used in an effort to prevent that outcome from occurring.

Source: Aggarwal & Reddie, 2018

International relations (IR)

For a school of IR realists the great powers will be driven to strive for hegemony, i.e., extending their **control**, either globally or at least regionally. Within strategic autonomy, control is essential and may

be realised in four ways: autarky (which is closest to hegemon thinking in case of the great powers), risk management, strategic partnerships of likeminded, and global commons with distributed control. Focusing on control in strategic partnerships, if this becomes one partner seeking to expand control at the expense of the other (e.g., by an America First policy or interpreting the intent for American leadership in 6G in an absolute sense) the partnership is bound to fail. If on the other hand control is seen as a common interest, i.e., control vis-à-vis third countries, room is created for an internal market in the partnership in which specialisation can thrive which would deliver large economic benefits (Figure 11 from (Boston Consulting Group & Semiconductor Industry Association, 2021)).

Figure 11 Cost savings in semiconductors by specialisation

This can only become a reality if there are safeguards, such as mutual guarantees to deal with shortages and continuity of two-way supply (Breton, 2022b), and otherwise credible promises. The approaches have been studied under international game theory by Nobel prize winner Thomas Schelling. Note that smaller countries and regions may have no choice but to specialise. The EU may be in that position too.

Recently scholars started to address not only the renewed interest in industrial policy but also its interplay with geopolitics and with technological change. For instance, (Giacomello et al., 2021) point to (digital) technology becoming a source of empowerment for states, while also stating that IR, international political economy, and security studies for technology innovation has often failed to recognise the importance of technological innovation and diffusion. The nexus of the evolution of the international environment and technological trends has been occasional investigated, although recently an emerging paradigm, still ill-defined, is **techno-politics** which has grown out of Science & Technology Studies and takes seriously a two-way interplay of technology and (international) politics[95].

A specific case is the interplay of technological and social construction, in particular of sovereignty[96]. Most IR scholars have considered technology as an exogenous factor, not as a central matter of inquiry and methodological debate. The exception is the internet, but the previous holds for most of the other digital technologies such as AI, semiconductors, cloud, etc. (Aiginger & Rodrik, 2020) take disruptive political and technological change as a given, and then identify several reasons for the renewal of industrial policy, such as the pushback against the 'Washington Consensus', the rise of China, and rising importance of societal and environmental goals. They also point in particular in Europe to the conflict between competition and industrial policy, the former in the short tun being more about consumer welfare, the latter about productive, dynamic industries – even if in the long run these goals ought to be consistent. Already here we can note that strategic autonomy may be top on the list for governments, the private sector may be less interested in this as a strategic intent, or even be against it when it is interpreted in a narrow protectionist and national sense. The term 'industrial' should not

[95] (Eriksson & Newlove-Eriksson, 2021).
[96] (Timmers, 2022a).

be understood as 'manufacturing'. It is here much wider. (Aiginger & Rodrik, 2020) see contemporary industrial policy as being less about to-do incentives as in the past but more about sustained private-public collaboration. They then give ten forms of guidance for industrial policy in the 21st century, from which we select 'industrial policy has to be systemic, not isolated, not delegated to specialists', 'societal goals to be paramount, beyond correcting market failures', 'industrial policy is a search process in unknown territory', and 'Asian countries demonstrate how to combine planning with market forces'. Finally, (E. Cohen, 2022) firmly links industrial policy to sovereignty.

Politics and international relations theory suggests that strategic alliances must have strategic intent, a long-term perspective, and always a national security dimension, that is, sovereignty always plays a role, explicitly or implicitly. However, academic work also makes clear that strategic alliances over the last 30 years still largely remain 'unidentified political objects'[97], that many partnerships exist only in intent but not in implementation, that there may be a weak or no alignment of normative and instrumental objectives, and that there is ample scope for ambiguity in strategic intent[98].

It is now increasingly and frequently reported that international standardisation (which is *par excellence* a tool of industrial policy, even in its low-interventionist forms) has been captured by geopolitics. The fight for the top position of the ITU between the Western democracy block and a Russia/China- candidate has the fingerprints of geopolitics all over it[99]. The fight has already played itself out in the UN as regards norms and values in cyberspace and is a telling story. First, the discussions forked into two groups, essentially on equal footing to report to the UN General Assembly. Next, one of the groups could conclude its work rapidly but only by dropping ideological debate on human-centricity and by not tackling accountability which raises great doubts about implementation. Work in the other group stalled due full-size polarisation triggered by the war in Ukraine (Hurel, 2022). It is only a matter of time before such fights will also show up in other standardisation forums, whether government-led (work within public health in WHO) as well as in industry-led platforms for mobile communications 5G/6G, IoT, confidential computing, and quantum computing. This is the reality of geopolitics *ab initio* conditioning industrial policy. This will also extend to international industry platforms such as for semiconductors or automotive or Internet of Things (IoT). Already in 2019 the founder of Huawei predicted that after 5G it would be IoT that would become the geopolitical/geoeconomic battleground[100].

Within political theories we find the interplay between government and business and technology developments affecting the governmental and policymaking system (also expressed as 'code is law' and 'law is code'). This interplay is also called governmentalism[101].

The geo-politisation of industry and technology interest groups, collaboration platforms, informal and formal norms and standards-setting groups, is unavoidable. Each of these will have to reflect now on

[97] Quoting from Tyushka, A., and Czechowska, L. (2019), who paraphrase Jacques Delors.
[98] (Tyushka & Czechowska, 2019).
[99] (Harcourt et al., 2020), (Baron & Kanevskaia Whitaker, 2021).
[100] (Yan et al., 2019).
[101] (J. E. Cohen, 2019; Timmers, 2022a).

choices to be made or be coerced into a choice.

National Competitiveness, Industrial Ecosystem

There is a rich literature on national (EU) competitiveness and industrial ecosystems. This includes the World Economic Forum Competitiveness Index and research on national competitiveness (Delgado et al., 2012), Michael Porter's Diamond Model[102], work on industrial and regional Clusters by Delgado, Porter and Stern[103] and generally the analysis of European industrial policy by (Bianchi & Labory, 2020). Furthermore insights into national innovation systems is provided by (Freeman & Soete, 1997), (Dosi et al., 1988) as well as (Kenney & Zysman, 2016). Zysman and Tyson also address public intervention for industrial transition. Finally for research on online platforms as economic infrastructures (two-sided markets) see (Codagnone et al., 2018).

Our entry point here to analyse national competitiveness is the commonly used Diamond model that Michael Porter developed in the 1980s and 1990s[104]. Though rather old, it remains usable and valid. It allows dynamics of forces and factors to be described in a 'narrative'. A brief explanation of the diagram used in Figure 7 'Porter model for national competitiveness':

- Factor conditions. The country's position as regards factors of production, such as skilled labour or infrastructure, which are necessary to compete in a given sector.
- Demand conditions. The nature of the demand on the home market for the product or service of the sector.
- Related and supporting industries. The presence or absence in the country of suppliers and other related industries that are internationally competitive.
- Firm strategy, structure and rivalry. The conditions in the nation that determine how companies are created, organised and managed, as well as the nature of domestic rivalry.

Business strategy and industrial economics

References here include transaction cost economics and contractual theory by (Williamson, 1985), business models and business strategy by (Teece, 2010; Timmers, 1998), network economy theory applied to the firm by (Shapiro & Varian, 1994), while online platform theory straddles the ground between industrial economics and industrial ecosystems (see below). Industrial dynamics has been studied by Schumpeter and the evolutionary approach of Nelson-Winter[105]. Insightful are the views of (Dosi, 2011) on decentralised disruptive and centralised demand management approaches to boost innovation, i.e., respectively Schumpeter and Keynes. Useful at firm-level is also Porter's Five Forces model, which is designed to analyse competitiveness in order to develop business strategy (see Figure 12). An excellent explanation is in the 2008 Harvard Business Review[106]. A brief description of the main elements, from the above reference, is:

- New entrant threat: new entrants put new capacity under pressure, prices, and investments.

[102] (Porter, 1990).
[103] (Delgado et al., 2014).
[104] https://www.isc.hbs.edu/competitiveness-economic-development/frameworks-and-key-concepts/Pages/default.aspx
[105] (Nelson & Winter, 1985).
[106] See: https://www.isc.hbs.edu/strategy/business-strategy/Pages/the-five-forces.aspx

- Powerful suppliers retain more value for themselves by raising prices, reducing quality, or transferring costs to customers.
- Authorised buyers are more valuable to themselves by pushing prices, demanding more quality or service, and playing vendors against each other.
- Threat of substitutes: These may replace the product by redoing the same function.
- Competition between existing competitors: can take various forms, such as discounts, advertisements, new products, and the improvement of services.

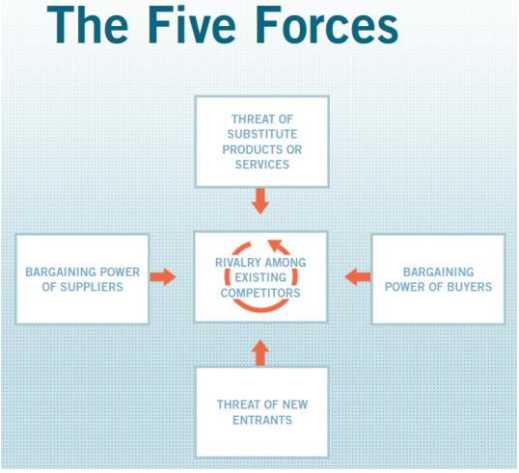


Figure 12: Five forces affecting firm-level competition

Alliances, partnerships, value chains

A common notion in the three perspectives is collaboration between one or more parties, i.e., alliances or partnerships or industrial co-operation. Digital tech alliances have been analysed in (Timmers, 2022b). Academic work makes clear that strategic alliances over the last 30 years still largely remain 'unidentified political objects'[107], that many partnerships exist only in intent but not in implementation, that there may be a weak or no alignment of normative and instrumental objectives, and that there is ample scope for ambiguity in strategic intent (Tyushka & Czechowska, 2019). Partnerships are a natural object of national competitiveness theory or industrial ecosystems, which is also rich in examples of mechanisms such as PPPs or regional clustering[108].

In industrial economics and business strategy, the concept of alliances and partnerships maps onto value chain relations, vertical and horizontal integration, and more generally onto business models[109]. Of particular importance are the developments enabled by the internet of two-sided collaboration through mediated platforms which have only become more important (platform economy see (Codagnone, 2022), and distributed collaboration mediated through blockchain (De Filippi & Wright, 2019).

[107] Quoting from Tyushka, A., and Czechowska, L. (2019), who paraphrase Jacques Delors.
[108] (Porter, 1990), (Delgado et al., 2012), (Bianchi, Patrizio & Labory, Sandrine, 2006).
[109] (Belussi et al., 2019).

ANNEX II: CASES IN DETAIL

More detail is provided below on EU digital industrial policies or policy actions relevant to the three cases.

Case: Semiconductor Policy and the EU Chips Act

The text below is based on a publication by the Brookings Institute[110].

The EU Chips Act launches a broad investment program along three lines of effort. The first pillar of the Act supports large-scale technological capacity building and innovation in cutting-edge chips. The second pillar provides large-scale investments in production capacities. The third pillar aims to improve the ability to spot and respond to semiconductor supply crises.

Pillar 1 includes a public-private partnership, the 'EU Chips Joint Undertaking', including 25 EU member states, Israel, Turkey, Norway, the European Commission, and hundreds of companies and research centres. This pillar addresses semiconductor research, semiconductor pilot production lines, standards, certification for energy-efficiency and security of chips, skills, and networking of semiconductor expertise centres. Its technological focus includes chips design, advanced node technology (sub-2 nm), and quantum chips. By focusing on new technological paradigms (quantum), advanced chip designs (sub-2 nm), and new production methods that bridge "from lab to fab", the first pillar aims to strengthen the EU's position in the semiconductor pre-production phase. It provides both research and innovation funding and seeks to strengthen the industrial ecosystem by networking competence centres that offer semiconductor expertise and skills development across Europe. It also provides venture funding through a new Chips Fund for start-ups, scale-ups, and smaller companies.

Pillar 2 enables setting up vertically integrated production facilities as well as 'Open EU Foundries' (fabs that produce for third parties chips designed by others). Both need to be "first-of-a-kind"—that is, they are not already present in the EU in terms of technology node, substrate material, or other product innovations that can offer better performance, process innovation, or energy and environmental performance. Companies can access State aid and direct EU and national funding mainly for new fab construction. They will also benefit from fast-tracked administrative permits.

Pillar 3 aims to ensure continuity of supply in case of a semiconductor crisis. This will be done by monitoring early warning indicators for shortages in chip supply relative to demand and escalation mechanisms to activate a semiconductor crisis stage. To head off a shortage, coordinated procurement can be carried out. Companies under the second pillar can also be requested to shift production towards the scarce critical semiconductors. Early warning indicators are being developed.

Using the policy action terminology above for the industrial ecosystem, the following actions are then pursued by the EU semiconductor policy (we define the fabs as the producers and all other companies as either suppliers or buyers):

[110] (Timmers, 2022c).

Table 5: Types of policy action, their object in the digital industrial ecosystem , EU semiconductor policy actions

Policy action type	Ecosystem object	EU Chips Act actions (for pillars see above)
Defining	Industrial ecosystem	Advanced chips + mature chips + quantum chips Industrial ecosystem – EU-wide, to some extent transatlantic
Creating	Partnerships	Pillar 1: Joint Undertaking, future European Chips Infrastructure Consortium
Substituting	Market	Pillar 3: Potential stockpiling
Facilitating	Suppliers Producers Suppliers Producers	Pillar 1: R&D support esp. for design, quantum Pillar 2: Network of competence centres Pillar 1: R&D support for new production methods Pillar 1: SME risk capital Chips Fund Pillar 2: State aid
Modifying	Suppliers Producers	Pillar 2: Security, low energy design requirements Pillar 2: Environmental conditions (especially for fabs)
Proscribing	Supply chain	Pillar 3: supply crisis interventions
External action	Fabs Supply chain	Pillar 2-related TTC action on subsidy races Pillar 3-related TTC action on chips shortages

As can be observed from the table, clearly most actions are ecosystem facilitating.

Case: Trusted Cloud and EU Cloud

Cloud R&D initiatives supported by EU funding have been running over many years. In 2019 the GAIA-X cloud initiative was launched, anchored in the private sector but strongly supported by France and Germany and subsequently joined by several other countries and many companies. GAIA-X emphasises interoperability, trusted cloud, and sectoral cloud solutions. GAIA-X provides for a common architecture, interoperability, privacy and security specifications, and a wide range of pilots, from cloud in health to manufacturing (Industry 4.0).

In parallel and very much in line with the direction set by GAIA-X EU-level cloud initiatives have been developed: cloud certification (supported by the EU's cybersecurity agency ENISA), trusted cloud services, and R&D. Given the dominance of cloud for data processing, EU cloud policy cannot be seen independent from EU data policy initiatives. These include support for European data spaces in a wide range of areas, and, importantly, data regulation in the EU notably the Data Governance Act and the Data Act, but also sectoral legislation such as for public sector information (Open Data Directive) and health data (European Health Data Space Regulation), and to some extent the portability requirements of the Digital Markets Act, the Free Flow of Non-Personal Data Regulation (FFoDR), and the GDPR, and even the proposed AI Act.

In the table below we label the producers as the cloud providers, suppliers are providing value added such as data analytics, trust/authentication, and security services.

Table 6: Types of policy action, their object in the digital industrial ecosystem , EU cloud policy actions

Policy action type	Ecosystem object	EU Cloud Policy actions
Defining	Cloud ecosystem Edge cloud ecosystem?	EU Data Policy (overall EU Cloud Policy does not yet exist) Defined by future EU edge cloud policy?
Creating	Market	Public sector information legislation
Substituting	Market	Data space policy, esp. public data spaces, EHDS
Transitioning	Ecosystem	Cloud -> Edge cloud, not likely, viz. edge cloud policy
Facilitating	Buyers Buyers Suppliers Market Market Market	FFoDR: data portability GDPR for personal data controllers: codes of conduct DGA: labelling of data intermediaries Horizon: EU R&D and piloting funding Digital Europe/CEF/RRF: funding cloud deployment, take-up GAIA-X; European Alliance for Industrial Data, Edge and Cloud
Modifying	Market	Cyber Act: cloud security schemes
Proscribing	Market Providers Providers	NIS2, DORA: mandatory cloud security DMA, DA: data portability, interoperability/cloud switching Competition policy: cloud competition cases
External	Providers, Buyers	Future: foreign law immunity requirements?

Case: Digital Identity and EU Digital Wallet

In 2014 after a lengthy negotiation the EU eIDAS regulation was adopted, which regulates the mutual recognition of national eID and e-Signatures across the internal market, as well as several additional trust or authentication services such as timestamping. eIDAS provides these services or functional a legal basis, meaning that they can be used as legal evidence. eIDAS furthermore arranges for the development of common interoperability specifications, which have been implemented in cross-border interconnect facilities, supported by funding from the Connecting Europe Facility, that technically enable the cross-border use of the eIDAS-recognised digital identity and other digital trust services.

eIDAS had a limited success in terms of take-up of national eID and related services (strong cases are ITSME in Belgium and the Estonian eID but some large countries notably Germany did not put forward a national eID). Moreover, in the meantime eID schemes driven by the tech giants have been entering at large scale daily use, to the extent that they have become in a number of cases the preferred way to identify as a citizen towards the government enabling citizen/consumer profiling by these companies, posing a challenge to state and individual sovereignty. Also, in the meantime the concept of a digital wallet had been developing, which allows to store a rich set of attributes associated with a citizen/consumer. A prime example then became the EU COVID-19 Pass, storing vaccination data (even if it can be criticised that it over-exposes personal data). Blockchain started to be seen as a technology that could enable greater control over personal data (self-sovereignty).

In 2021 then the European Commission proposed a legislative update, the eIDAS2 or EU Digital Wallet Regulation, to respond to these developments. The Regulation is foreseen to be adopted in 2023. Accompanying, as before, are pilots and cross-border services, supported by the Digital Europe and CEF programmes. The proposed Regulation is back-to-back with the DMA where it concerns using national eIDs (eIDAS eIDs) as a means to identify for access to social media and cloud services that cannot be refused by the platform provider.

Moreover, the European infrastructure for eID interoperability is supported by the CEF program. In addition, the EU Digital Wallet is being implemented by a federation of national digital wallets that are interoperable, their interoperability infrastructure, and blockchain supported credentials management. The latter can be based on a self-sovereign approach. EU funding from the Digital Europe Programme support the piloting and roll-out of this federating approach, the EU Digital Wallet.

EU digital government policy (such as a range of EU's eGovernment Action Plans and the eIDAS Regulation) offers consistent support over nearly 20 years to extend the use of nationally recognised eIDs that have also been notified at European level (and can therefore be used interoperably across the EU). The EU also is actively promoting eIDAS approach in international co-operation, including in the Global Gateway programme, and in international standardisation such as in ITU and trade facilitation such as UNCITRAL and sectoral use of eIDAS notably in banking (for Know Your Customer KYC requirements).

Table 7: Types of policy action, their object in the digital industrial ecosystem, EU digital identity policy actions

Policy action type	Ecosystem object	Digital Identity Policy actions
Defining	Digital identity ecosystem	An EU industrial policy still needs to be formulated
Creating	Market	National eID required for public services (COVID-19 Pass) Future: EU-wide services accessed with EU Digital Wallet
Substituting	-	-
Transitioning	Ecosystem	Digital transition policies for paper-based trust services
Facilitating		Digital Europe/CEF/RRF: funding EU Digital Wallet deployment, take-up, link to EU blockchain infrastructure
Modifying	Market	eIDAS: security schemes
Proscribing	Providers, Buyers	eIDAS: only notified eIDs of high-security level are legally EU-wide; idem for trust services such as e-signatures
External	Providers, Buyers	UN potential model law Future: only national eID/Wallet for sovereign functions of the state (public services, voting, etc).

The table above shows, at the same time, the basic problem of lack of an industrial policy for digital identity and the opportunity created by several policy actions already being in place.

REFERENCES

Accenture. (2022, February 1). *The Power of the Semiconductor Value Chain | Accenture*. https://www.accenture.com/us-en/insights/high-tech/semi-value-chain

Aggarwal, V. K., & Reddie, A. W. (2018). Comparative industrial policy and cybersecurity: A framework for analysis. *Https://Doi.Org/10.1080/23738871.2018.1553989*, *3*(3), 291–305. https://doi.org/10.1080/23738871.2018.1553989

Aiginger, K., & Rodrik, D. (2020). Rebirth of Industrial Policy and an Agenda for the Twenty-First Century. *Journal of Industry, Competition and Trade*, *20*(2), 189–207. https://doi.org/10.1007/s10842-019-00322-3

Anderson, J. (2022). *Europe needs high-tech talent:* (Strategic Autonomy Series). FEPS. https://feps-europe.eu/publication/europe-needs-high-tech/

Art, R. J., & Jervis, R. (2016). *International Politics: Enduring Concepts and Contemporary Issues* (13th edition). Pearson.

ASML. (2022). *EU Chips Act Position paper*.

Banet, C., Pollitt, M., Covatariu, A., & Duma, D. (2021, October). Data Centres and the Grid – Greening ICT in Europe | CERRE Report. *CERRE*. https://cerre.eu/publications/data-centres-and-the-energy-grid/

Barlow, J. P. (1996, February 8). *A Declaration of the Independence of Cyberspace*. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Baron, J., & Kanevskaia Whitaker, O. (2021). Global Competition for Leadership Positions in Standards Development Organizations. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3818143

Baron, J., & Larouche, P. (CERRE, forthcoming). *The European Standardisation System at a crossroads | CERRE*. CERRE.

Belussi, F., Orsi, L., & Savarese, M. (2019). Mapping Business Model Research: A Document Bibliometric Analysis. *Scandinavian Journal of Management*, *35*(3), 101048. https://doi.org/10.1016/j.scaman.2019.101048

Berkeley Engineering. (2021, June 17). *Berkeley engineering students pull off novel chip design in a single semester*. Berkeley Engineering. https://engineering.berkeley.edu/news/2021/06/berkeley-engineering-students-design-novel-chip-in-semester-long-course/

Bianchi, P., & Labory, S. (2020). European Industrial Policy: A Comparative Perspective. In A. Oqubay, C. Cramer, H.-J. Chang, & R. Kozul-Wright (Eds.), *The Oxford Handbook of Industrial Policy* (pp. 593–620). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198862420.013.22

Bianchi, Patrizio, & Labory, Sandrine. (2006). *International Handbook on Industrial Policy*. Edward Elgar Publishing. https://www.e-elgar.com/shop/usd/international-handbook-on-industrial-policy-9781843768364.html

Bickerton, C., Brack, N., Coman, R., & Crespy, A. (2022). Conflicts of sovereignty in contemporary Europe: A framework of analysis. *Comparative European Politics*, *20*(3), 257–274. https://doi.org/10.1057/s41295-022-00269-6

Biersteker, T. (2012). State, Sovereignty and Territory. In W. Carlsnaes, T. Risse, & B. A. Simmons, *Handbook of International Relations*. SAGE Publications Ltd.

Boston Consulting Group & Semiconductor Industry Association. (2021). *Strengthening the Global Semiconductor Supply Chain in an Uncertain Era | BCG*. https://www.bcg.com/publications/2021/strengthening-the-global-semiconductor-supply-chain

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*.

Breton, T. (2022a, July 5). *Sneak peek: How the Commission will enforce the DSA & DMA | LinkedIn*. https://www.linkedin.com/pulse/sneak-peek-how-commission-enforce-dsa-dma-thierry-breton/?trackingId=tXe8d2cmRD6IELMZDYOuaQ%3D%3D

Breton, T. (2022b, September 6). Speech by Commissioner Thierry Breton: Sovereignty, self-assurance and solidarity: Europe in today's geopolitics. *PubAffairs Bruxelles*. https://www.pubaffairsbruxelles.eu/eu-institution-news/speech-by-commissioner-thierry-breton-sovereignty-self-assurance-and-solidarity-europe-in-todays-geopolitics/

Carretero, R. (2022, October 5). Dynamic competition, the trendy concept in Brussels and Spain policy debates. *Telefónica*. https://www.telefonica.com/en/communication-room/blog/dynamic-competition-the-trendy-concept-in-brussels-and-spain-policy-debates/

Chakraborty, S. (2022, March 1). *The Semiconductor Shortage Explained*. Electronics & Semiconductors. https://blogs.sw.siemens.com/electronics-semiconductors/2022/03/01/the-semiconductor-shortage-explained/

China Technology Forecast in 2025: Fragile Tech Superpower. (2020, October 26). MacroPolo. https://macropolo.org/analysis/china-technology-forecast-2025-fragile-tech-superpower/

Codagnone, C. (2022). The Platform Economy After COVID-19: Regulation and the Precautionary Principle. In H. Werthner, E. Prem, E. A. Lee, & C. Ghezzi (Eds.), *Perspectives on Digital Humanism* (pp. 173–179). Springer International Publishing. https://doi.org/10.1007/978-3-030-86144-5_24

Codagnone, C., Matthews, J., & Karatzogianni, A. (2018). *Platform Economics: Rhetoric and Reality in the 'Sharing Economy'*. Emerald Publishing.

Cohen, E. (2022). *Souveraineté industrielle. Vers un nouveau modèle productif*. http://www.elie-cohen.eu/Souverainete-industrielle-Vers-un-nouveau-modele-productif.html

Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism*.

Council of the European Union. (2022, December 1). *Chips Act: Council adopts position*. https://www.consilium.europa.eu/en/press/press-releases/2022/12/01/chips-act-council-adopts-position/

Council on Foreign Relations. (2022, July 12). *The United States Needs a New Foreign Policy for Cyberspace*. Council on Foreign Relations. https://www.cfr.org/report/confronting-reality-in-cyberspace

Coyle, D., & Muhtar, A. (2021). *Industrial Policy: Learning from the past*. University of Cambridge. https://www.bennettinstitute.cam.ac.uk/publications/industrial-policy-learning-past/

de Bruin, L. (2018, June 18). Porter's Diamond Model EXPLAINED with EXAMPLES | B2U. *B2U - Business-to-You.Com*. https://www.business-to-you.com/porter-diamond-model/

De Filippi, P., & Wright, A. (2019). *Blockchain and the Law*. Harvard University Press. https://www.hup.harvard.edu/catalog.php?isbn=9780674241596

Delgado, M., Ketels, C., Porter, M. E., & Stern, S. (2012). *The Determinants of National Competitiveness* (Working Paper No. 18249). National Bureau of Economic Research. https://doi.org/10.3386/w18249

Delgado, M., Porter, M. E., & Stern, S. (2014). Clusters, convergence, and economic performance. *Research Policy*, *43*(10), 1785–1799. https://doi.org/10.1016/j.respol.2014.05.007

Dobberstein, L. (2022, November 7). *China likely is stockpiling vulnerabilities, says Microsoft*. https://www.theregister.com/2022/11/07/china_stockpiles_vulnerabilities_microsoft_asserts/

Dosi, G. (2011). Giovanni Dosi: Combining Schumpeter and Keynes to Boost Innovation. *Joseph Schumpeter*. https://contemporarythinkers.org/schumpeter/multimedia/giovanni-dosi-combining-schumpeter-and-keynes-to-boost-innovation/

Dosi, G., Freeman, C., Nelson, R., Silverberg, G., & Soete, L. (1988). *Technical change and economic theory*. Laboratory of Economics and Management (LEM), Sant'Anna School of Advanced ….

Eriksson, J., & Newlove-Eriksson, L. M. (2021). Theorizing technology and international relations: Prevailing perspectives and new horizons. *Technology and International Relations*, 3–22.

European Commission. (2019, January 2). *Overview of pre-notified and notified eID schemes under eIDAS - eID User Community -*. https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

European Commission. (2020a). *FDI screening | DG TRADE*. https://trade.ec.europa.eu/access-to-markets/en/content/fdi-screening

European Commission. (2020b). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0595

European Commission. (2021a, February 18). *An open, sustainable and assertive trade policy* [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_645

European Commission. (2021b, May 5). *Updating the 2020 industrial strategy: Towards a stronger single market for Europe's recovery, COM(2021)350*. https://ec.europa.eu/growth/news/updating-2020-industrial-strategy-towards-stronger-single-market-europes-recovery-2021-05-05_en

European Commission. (2021c, October 18). *The EU Digital COVID Certificate: EU has set a standard*. Press Release. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_5267

Communication from the Commission Criteria for the analysis of the compatibility with the internal market of State aid to promote the execution of important projects of common European interest 2021/C 528/02, no. C/2021/8481 (2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.C_.2021.528.01.0010.01.ENG&toc=OJ%3AC%3A2021%3A528%3ATOC

European Commission. (2021d, December 30). *IPCEI*. https://competition-policy.ec.europa.eu/state-aid/legislation/modernisation/ipcei_en

A Chips Act for Europe, European Commission (2022) (testimony of European Commission). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0045&qid=1664190455505

European Commission. (2022). *European Chips Act: Staff Working document | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/library/european-chips-act-staff-working-document

Freeman, C., & Soete, L. (1997). *The Economics of Industrial Innovation—3rd Edition* (third edition). MIT Press.

French and German Governments. (2019). *A Franco-German Manifesto for a European industrial policy fit for the 21st Century*. https://www.bmwk.de/SiteGlobals/BMWI/Forms/Suche/DE/Servicesuche_Formular.html?resourceId=180050&input_=807920&pageLocale=de&selectSort=score+desc&templateQueryStringListen=manifesto

Friedrichs, J., & Kratochwil, F. (2009). On Acting and Knowing: How Pragmatism Can Advance International Relations Research and Methodology. *International Organization*, *63*(4), 701–731. https://doi.org/10.1017/S0020818309990142

Giacomello, G., Moro, F. N., & Valigi, M. (Eds.). (2021). *Technology and International Relations: The New Frontier in Global Power*. Edward Elgar Publishing.

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M.-G., Bômont, C., Braun, M., Danet, D., Disforges, A., Géry, A., Grumbach, S., Hummel, P., Limonier, K., Münßinger, M., Nicolai, F., Pétiniaud, L., Winkler, J., & Zanin, C. (2022). Contested Spatialities of Digital Sovereignty. *Geopolitics*, *XX*(X), 1–40. https://doi.org/10.1080/14650045.2022.2050070

Harcourt, A., Christou, G., & Simpson, S. (2020). Global Standard Setting in Internet Governance. In A. Harcourt, G. Christou, & S. Simpson, *Global Standard Setting in Internet Governance*. Oxford University Press. https://doi.org/10.1093/oso/9780198841524.003.0005

Heidegger, M. (1977). *Question Concerning Technology, and Other Essays, The* (12.2.1976 edition). Harper Torchbooks.

Hofer, J., & Scheuer, S. (2022, September 28). *iPhone-Hersteller: Apple-Chef Tim Cook in München: Ingenieure sollen riskante Schwäche bei 5G beheben | Handelsblatt*. https://www.handelsblatt.com/technik/it-internet/iphone-hersteller-apple-chef-tim-cook-in-muenchen-ingenieure-sollen-riskante-schwaeche-bei-5g-beheben/28709150.html

Hurel, L. M. (2022, September 6). *The Rocky Road to Cyber Norms at the United Nations*. Council on Foreign Relations. https://www.cfr.org/blog/rocky-road-cyber-norms-united-nations-0

Ji-hyoung, S. (2022, January 24). *[Korea Chips Act] Korea sets out own Chips Act, in less ambitious fashion*. The Korea Herald. https://www.koreaherald.com/view.php?ud=20220124000671

Jones, M. D., & McBeth, M. K. (2010). A Narrative Policy Framework: Clear Enough to Be Wrong? *Policy Studies Journal*, *38*(2), 329–353. https://doi.org/10.1111/j.1541-0072.2010.00364.x

Kayali, L., & Eder, F. (2020, September 1). *Thierry Breton 'understands' Trump on TikTok, wants data stored in Europe*. POLITICO. https://www.politico.eu/article/breton-wants-tiktok-data-to-stay-in-europe/

Kearney. (2021). *Europe's urgent need to invest in a leading-edge semiconductor ecosystem*.

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Kenney, M., & Zysman, J. (2016). The rise of the platform economy. *Issues in Science and Technology*, *32*(3), 61.

Klabbers, J. (2021). *International Law* (3rd edition). Cambridge University Press.

Kleinhans, J.-P. (2021). The lack of semiconductor manufacturing in Europe. In *SNV Policy Briefs*.

KPMG France. (2021, May 25). *The European Cloud industry: A market worth €300bn+ by 2027-2030. Could half of this potential growth slip through Europe's hands?* https://corporate.ovhcloud.com/en/newsroom/news/europe-cloud-challenges-key-and-five-scenarios-impact/

Lambert, F. (2021, January 25). *Tesla partners with Samsung on new 5nm chip for full self-driving, report says*. Electrek. https://electrek.co/2021/01/25/tesla-partners-samsung-new-5nm-chip-full-self-driving-report/

Lessig, Lawrence. (1999). *Code: And Other Laws Of Cyberspace*. Basic Books.

Lewis, W. W. (2005). *The Power of Productivity: Wealth, Poverty, and the Threat to Global Stability*. University of Chicago Press.

Matishak, M. (2022, September 28). Senate panel approves open-source software bill, though future unclear. *The Record by Recorded Future*. https://www-therecord.recfut.com/senate-panel-approves-open-source-software-bill-though-future-unclear/

Mazzucato, M., & Kattel, R. (2020). *Grand Challenges, Industrial Policy, and Public Value*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198862420.013.12

McKinsey. (2022, August 24). *Technology Trends Outlook 2022*. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech?stcr=613FE23AE98C418CBE93BE4DBC78149A&cid=other-eml-ttn-mip-mck&hlkid=9cfd7c33c1054da6a05e1342d916a293&hctky=12587447&hdpid=4152e07e-e036-43ac-aae6-581bf29a305c

Miller, C. (2022). *Chip War*. Scribner. https://www.christophermiller.net/semiconductors-1

Murphy, B. (2022, May). Chokepoints—China's Self-Identified Strategic Technology Import Dependencies. *Center for Security and Emerging Technology*. https://cset.georgetown.edu/publication/chokepoints/

NCSC-NL. (2022a, August 16). *How the CLOUD-Act works in data storage in Europe—By our experts—National Cyber Security Centre* [Webpagina]. Nationaal Cyber Security Centrum. https://english.ncsc.nl/latest/weblog/weblog/2022/how-the-cloud-act-works-in-data-storage-in-europe

NCSC-NL. (2022b, November 23). *'Kleine kans' dat Amerikaanse overheid toegang krijgt tot Europese gegevens op basis van de CLOUD-Act—Expertblogs—Nationaal Cyber Security Centrum* [Webpagina]. Nationaal Cyber Security Centrum. https://www.ncsc.nl/actueel/weblog/weblog/2022/kleine-kans-dat-amerikaanse-overheid-toegang-krijgt-tot-europese-gegevens-op-basis-van-de-cloud-act

Nelson, R. R., & Winter, S. G. (1985). *An Evolutionary Theory of Economic Change*. Belknap Press: An Imprint of Harvard University Press.

NICA, D. (2022, September 19). *DRAFT REPORT on the proposal for a regulation of the European Parliament and of the Council Establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act) | ITRE_PR(2022)731655 | European Parliament*. https://www.europarl.europa.eu/doceo/document/ITRE-PR-731655_EN.html

Nielsen, C., & Lund, M. (2014). An Introduction to Business Models. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2579454

NXP. (2022, September 30). *NXP warns EU microchips funding falls far behind 2030 targets | Politico*. POLITICO. https://www.politico.eu/article/microchips-maker-nxp-warns-eu-chips-funding-falls-far-behind-its-2030-targets/

Peters, G. C. (2022, September 28). *S.4913 - 117th Congress (2021-2022): Securing Open Source Software Act of 2022* (2021/2022) [Webpage]. http://www.congress.gov/

Poitiers, N., & Weil, P. (2022, January 26). *Opaque and ill-defined: The problems with Europe's IPCEI subsidy framework | Bruegel blog*. Bruegel | The Brussels-Based Economic Think Tank. https://www.bruegel.org/blog-post/opaque-and-ill-defined-problems-europes-ipcei-subsidy-framework

Porter, M. E. (1990, March 1). The Competitive Advantage of Nations. *Harvard Business Review*. https://hbr.org/1990/03/the-competitive-advantage-of-nations

Reed, J. (2022, September 1). India's high-stakes bid to join the global semiconductor race. *Financial Times*.

Renda, A. (2022). *Leveraging digital regulation for Strategic Autonomy*. FEPS. https://www.feps-europe.eu/resources/publications/853-beyond-the-brussels-effect.html

Ritchie, H., & Roser, M. (2019). Technology Adoption. *Our World in Data*. https://ourworldindata.org/technology-adoption

Rodrik, D. (2022, June 6). *He predicted globalization's failure, now he's planning what's next—PolicyCast*. https://www.hks.harvard.edu/faculty-research/policycast/he-predicted-globalisms-failure-now-hes-planning-whats-next

Senate RPC. (2021, January 29). *The SolarWinds Cyberattack*. https://www.rpc.senate.gov/policy-papers/the-solarwinds-cyberattack

Shapiro, C., & Varian, H. (1994). *Information Rules: A Strategic Guide to the Network Economy* (8302nd edition). Hardcover.

Stefan Sagebro. (2022, June 10). *IPCEI - a lot of talk and a slow workshop*. Svenskt Näringsliv. https://www.svensktnaringsliv.se/english/ipcei-a-lot-of-talk-and-a-slow-workshop_1186847.html

Stocker, V., Knieps, G., & Dietzel, C. (2021). *The Rise and Evolution of Clouds and Private Networks – Internet Interconnection, Ecosystem Fragmentation* (SSRN Scholarly Paper ID 3910108). Social Science Research Network. https://doi.org/10.2139/ssrn.3910108

Teece, D. J. (2010). Business Models, Business Strategy and Innovation. *Long Range Planning*, *43*(2), 172–194. https://doi.org/10.1016/j.lrp.2009.07.003

The White House. (2022, September 6). *Press Briefing by Press Secretary Karine Jean-Pierre and Commerce Secretary Gina Raimondo*. The White House. https://www.whitehouse.gov/briefing-room/press-briefings/2022/09/06/press-briefing-by-press-secretary-karine-jean-pierre-and-commerce-secretary-gina-raimondo/

Thole, H. (2020, June 30). *Het kabinet steekt €20 miljoen in het Eindhovense Smart Photonics om te voorkomen dat de technologie in Aziatische handen valt*. Business Insider Nederland. https://www.businessinsider.nl/smart-photonics-kabinet-investering/

Timmers, P. (1998). Business Models for Electronic Markets. *Electronic Markets*, *8*(2), 3–8. https://doi.org/10.1080/10196789800000016

Timmers, P. (2018). The European Union's cybersecurity industrial policy. *Journal of Cyber Policy*, *3*(3), 363–384. https://doi.org/10.1080/23738871.2018.1562560

Timmers, P. (2021, July 23). *Debunking Strategic Autonomy » directions blog*. https://directionsblog.eu/debunking-strategic-autonomy/

Timmers, P. (2022a). The Technological Construction of Sovereignty. In *Perspectives on Digital Humanism* (pp. 213–218). Springer, Cham. https://doi.org/10.1007/978-3-030-86144-5_28

Timmers, P. (2022b). Strategic Autonomy Tech Alliances. *FEPS Strategic Autonomy Series*. https://www.feps-europe.eu/attachments/publications/220331%20final_strategic%20autonomy%20tech%20alliances-3a.pdf

Timmers, P. (2022c, August 9). How Europe aims to achieve strategic autonomy for semiconductors. *Brookings Tech Stream*. https://www.brookings.edu/techstream/how-europe-aims-to-achieve-strategic-autonomy-for-semiconductors/

Toet, D. (2022, July 22). *Een op drie ict-beslissers overweegt Europese cloud*. Computable. https://www.computable.nl/artikel/nieuws/cloud-computing/7389234/250449/een-op-drie-ict-beslissers-overweegt-europese-cloud.html

Tyushka, A., & Czechowska, L. (2019). Strategic partnerships, international politics and IR theory. *States, International Organizations and Strategic Partnerships*, 8–43. https://doi.org/10.4337/9781788972284.00010

US Congress. (2022, August 9). *CHIPS and Science Act*. https://www.govinfo.gov/content/pkg/PLAW-117publ167/html/PLAW-117publ167.htm

van Wijnen, J. F., Vleugels, A., & van Gils, S. (2022, September 25). *Hoge stroomprijzen drijven Nederlandse internetsector in armen van big tech | FD.nl*. FD.nl. https://fd.nl/bedrijfsleven/1451786/hoge-stroomprijzen-drijven-nederlandse-internetsector-in-armen-van-big-tech

Vodafone. (2022). *Open Strategic Sovereignty*. https://www.vodafone.com/sites/default/files/2022-03/open-strategic-sovereignty.pdf

Voelsen, D. (2019). *Cracks in the Internet's Foundation*. https://www.swp-berlin.org/en/publication/cracks-in-the-internets-foundation

von der Leyen, U. (2022, September 14). *State of the Union Address by President von der Leyen* [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_22_5493

Waters, R. (2022, November 13). US chipmakers reel from sharp boom to bust. *Financial Times*.

Williamson, O. E. (1985). *The Economic Institutions of Capitalism*. Free Press.

World Economic Forum. (2019). *Shaping the Future of Digital Economy and New Value Creation*. World Economic Forum. https://www.weforum.org/platforms/shaping-the-future-of-digital-economy-and-new-value-creation/

Yan, Y., Wong, S.-L., & Liu, N. (2019, July 4). Huawei founder predicts internet of things is next US battle—FT. *Financial Times*.

Yu, Y., Ting-Fang, C., & Li, L. (2022, June 5). From somebody to nobody: TSMC faces uphill battle in US talent war. *Financial Times*.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (First edition). PublicAffairs.

Zwetsloot, R., Corrigan, J., Weinstein, E., Peterson, D., Gehlhaus, D., & Fedasiuk, R. (2021). *China is Fast Outpacing U.S. STEM PhD Growth*. Center for Security and Emerging Technology. https://doi.org/10.51593/20210018

cerre Centre on Regulation in Europe

Avenue Louise 475 (box 10)
1050 Brussels, Belgium
+32 2 230 83 60
info@cerre.eu
www.cerre.eu
@CERRE_ThinkTank
Centre on Regulation in Europe (CERRE)
CERRE Think Tank