

# DGAP REPORT

THIS VOLUME IS THE THIRD OF FOUR MONITORING STUDIES

## The Digital Technology Environment and Europe's Capacity to Act



**Tyson Barker**  
Head of the Technology &  
Global Affairs Program



## IDEENWERKSTATT DEUTSCHE AUSSENPOLITIK

This monitoring study was written within the framework of the project “Ideenwerkstatt Deutsche Außenpolitik,” a process of reflection on the capacity to act in German and European foreign policy, the underlying conditions for which are undergoing a fundamental transformation. In addition to the much-discussed changes to the international system and increasing great-power competition between the United States and China, technological developments, new security threats, the consequences of climate change, and socio-economic upheaval are just some of the developments that will determine the future tasks and international impact of German foreign policy. Furthermore, the COVID-19 pandemic poses numerous political, economic, and societal risks; it accelerates many existing trends in the multilateral system with immediate consequences for Germany and the EU. In light of these challenges, the project “Ideenwerkstatt Deutsche Außenpolitik” aims to put German foreign policy to the test – through evidence-based analyses and interdisciplinary strategy discussions – and contribute to strengthening Germany's and the EU's capacity to act in foreign policy.

The project focuses on four thematic areas that are highly relevant for the future ability to act of German and European foreign policy: geo-economics, migration, security and defense, and technology. As part of the project's overall strategic and analytical effort, DGAP produce a monitoring study on each of these areas – four in total, including this one. All four studies analyze Europe's capacity to act and provide recommendations for EU and German policymakers on how to strengthen this capacity. In order to provide a nuanced yet comprehensive picture, they take into account

the different stages of the policy cycle: (1) problem definition, (2) agenda-setting, (3) policy formulation, (4) implementation, and (5) impact assessment. In gauging Europe's capacity to act, the studies refer to a series of scenario workshops on the four thematic areas, held in late 2020, in which DGAP and external experts created status-quo, best-case, and worst-case scenarios for how the future might look in 2030. Taking these respective scenarios into account, the monitoring studies analyze to what extent the EU and Germany are prepared for the worst case, are aware of the implications of the status quo, and are moving toward achieving the best case. The report that distills the results of the scenario workshops and all four monitoring studies can be found here:

<https://dgap.org/en/ideenwerkstatt-aussenpolitik>

This study on capacity to act in digital technology owes an immense debt of gratitude to a number of individuals without whom it would not have been possible. Thanks to Lucas Wollny, Martin Kümmel, Marlon Ebert, Richard Griefse, David Hagebölling, Jonas Winkel, Diego von Lieres and Becca Hunziker for their research, editing, advice and assistance with graphics. Also, to the team that lead this project: Roderick Parkes, Anna-Lena Kirch, and Serafine Dinkel for their coordination, persistence, and imagination, as well as John-Joseph Wilkins, Austin Davis Wiebke Ewering, Carl-Friedrich Richter and Helga Beck for editing and layout. Great appreciation also goes to Johannes Gabriel for his organization of the scenario workshop, and to the participants who gave up three days over Zoom to provide the raw material for the foresight analysis. Thanks also to Thorsten Klassen, Steffen Zorn, and Alicia von Voß for their efforts to make this project possible, as well as Daniela Schwarzer, Cathryn Clüver-Ashbrook, and Christian Mölling for their leadership.

This project is funded by

STIFTUNG  
MERCATOR

---

# Table of Contents

<b>Executive Summary</b>	<b>4</b>
<b>The Digital Environment and Europe's Capacity to Act</b>	<b>7</b>
<b>Three Scenarios for the Digital Environment in 2030</b>	<b>7</b>
<b>Measuring the EU's Capacity to Act Across Five Benchmarks</b>	<b>9</b>
Problem Definition	9
Agenda-Setting	12
Policy Formulation	14
Policy Implementation	16
Impact Capacity	21
<b>Germany's Role with Regard to the EU's Capacity to Act</b>	<b>23</b>
<b>Stocktaking: Assessment of Capacity to Act as a Whole</b>	<b>24</b>
<b>Implications and Recommendations Derived from the Monitoring Exercise</b>	<b>26</b>

---

**Digital technology has become a key dimension of geopolitical, economic, and normative power with states like China and the United States racing to claim the mantle of technological leadership. Others like Canada, Israel, Japan, and the UK are following. The EU has recognized that the instruments at its disposal are increasingly limited to its regulatory power, leveraging the desire of technology actors to access the vast European market. But relative market-size decline and steady erosion of innovation vis-à-vis peer competitors – even on Europe’s own competitive turf (automobiles, appliances, and industrial Internet of Things (IIoT)) – are beginning to take a heavier toll on Europe’s strategic outlook toward 2030. This has significant – and often still underappreciated – geopolitical implications for Europe’s future.**

As the EU has moved from a narrative around the Digital Single Market (DSM) to one around digital sovereignty, leaders have seen a growth in defensive action aimed at managing digital spaces – particularly in information and communication technology services (ICT) – and a new jolt of tech-industrial policy activity, most recently seen in the pandemic-inspired Recovery and Resilience Facility (RFF). The European Union has begun to coalesce around the notion of “digital sovereignty” as the leitmotif of its efforts, but has yet to tackle shades of difference between key players. The quest for digital sovereignty, which combines narrative power with rhetorical ambiguity, can at times paper over hard choices about strategic policy objectives, particularly between France and Germany, for the sake of consensus building.

Six realities frame the EU’s approach as it tries to forge unity for a more forceful, geopolitically-minded digital tech policy. First, Europe’s digital market remains fragmented. Second, technology itself has taken on a more general-purpose nature, with applications across sectors. Third, the geopolitical environment – particularly US-China tech competition – has raised the potential for the development of separate technology stacks. Fourth, the coronavirus pandemic has fueled the acceleration of Europe’s digital dependences on external actors and consolidated the dominance of Big Tech. Fifth, there has been a global renaissance in tech industrial policy. And finally, data governance is an increasingly contested space with the specter of digital localization looming large.

Overall, the 2030 baseline scenario points to a stagnant, negatively inflected trajectory for Europe if the EU continues to rest on its standing as a regulatory power. For the EU to redirect this trajectory to the best-case-scenario, ten policy objectives are central: complete the DSM; guarantee supply-chain access and resilience at all layers of the technology stack; establish leadership and control of critical and emerging technology areas; develop deep, interoperable, easily accessible data pools; unlock state, institutional, and venture capital (VC) investment; attract global ICT talent; conduct and commercialize emerging technology research and development (R&D); broaden global regulatory and standard-setting leadership beyond personal data and competition; strengthen cybersecurity; and advance reliable tech alliances with like-minded states.

The geopolitical environment – whether collaborative, hostile, or hybrid – is seen as an equally relevant factor in the EU’s ability to develop technological capacity. A benign geopolitical environment with consensus-driven, interoperable, and universally accepted tech standards, and governance would be most advantageous. Absent that, collaborative efforts with the United States, for instance in the Trade and Technology Council, could bolster Europe’s digital tech outlook.

For Germany, this means addressing the willingness to approach tech industrial policy – with meaningful investments in artificial intelligence (AI), quantum computing, semiconductors, and elsewhere – as truly European, rather than German projects. Germany will still shape European – and global – digital regulation by anticipating the EU’s tech regulatory agenda and establishing national laws, regulation, and standards that can then be elevated to the EU level. It has already done so in content moderation, digital competition, cybersecurity, and elsewhere.

Ultimately, the EU’s policy success will be determined by its ability to shore up areas where it is weakest – namely, improving policy formulation, implementation, and impact at home; and establishing constant and interactive benchmarking, honest performance assessments – particularly of failures – and confrontations with tradeoffs, particularly around regulation in areas like data governance, platform regulation, and AI. The EU must set out clearly defined objectives that confront the tough questions of “what is essential” and “what is nice to have.”

---

# The Digital Environment and Europe's Capacity to Act

In her 2020 State of the European Union address, European Commission President Ursula von der Leyen called the path to 2030 Europe's "digital decade." The EU introduced major new ideas on competition instruments, cloud computing, 5/6G, online media pluralism, election systems integrity, disinformation, platform regulation, and cybersecurity in 2020 with other major proposals on industrial data and AI planned for 2021. At the same time, the COVID-19 crisis has led states to look at major investments in emerging tech as part of national stimulus packages, and von der Leyen pledged that 20 percent of the EU's €750-billion recovery plan, NextGenerationEU, would go to making the continent ready for the deep digital age.

Taken together, the EU and its member states are undergoing a massive rethink on technology's impact on their economy, security, and democracy. As technological competitiveness moves from precision-centric engineering, as in the automotive sector, to data-centric analytics and user interfaces, there is a perception that the EU is falling behind. And von der Leyen's quest to transform the European Commission into a geopolitical body recognizes that a comprehensive approach to digital technology will be one of – if not the – most important determinants of Europe's ability to project power and global influence in the world of 2030.

But the way the EU uses the term "technology" in fact encompasses many very different policy areas. Even narrowly defined, technology includes areas as varied as semiconductor manufacturing, digital infrastructure, platform governance, e-commerce, artificial intelligence, cloud computing, quantum computing, the IoT, cybersecurity, and both personal and non-personal data. In recent European debates, it has even been broadened to include e-health, the future of work, smart cities, automated manufacturing, fintech, logistics, and, increasingly, the application of strategic technology in military contexts, just to name a few.

This high degree of complexity makes streamlined thinking about the efficacy of European tech policy immensely difficult – and one of the primary reasons that a series of successfully implemented policies does not always result in the ultimate outcomes the EU desires. The EU has had some success in exercising its capacity to act by setting global standards in privacy, competition, telecommunications, and internet protocols. Its gaming, IoT, and industrial internet sectors continue to stand among global tech leaders. All contribute to the EU's role as an exporter of both values and innovation.

At the same time, the EU has also had significant disappointments. Once dominant in the cellular handset market, European leadership in this area collapsed following the post-2007 smartphone boom. Earlier efforts to develop an indigenous PC industry and internet search have been unsuccessful. Europe is falling behind in AI adoption. The cloud market is being ceded to external actors. And Europe is increasingly dependent on external actors for the fabrication of chips – a key component for European manufacturing of cars, heavy machinery, and appliances. The Commission, member states, and industry are in the midst of demarcating sectors where leadership by other states is hard to contest and likely less central for future European technological power (PCs, social media platforms) from other areas where European tech industrial capacity will be determinant in the EU's future ability to secure its tech industrial base (in cloud computing and industrial data, for instance).

In some ways, Europe's efforts to coordinate digital tech policy are akin to conducting a symphony orchestra. The actors and mechanisms – regulatory, industrial, and market access-based – similar to instrumental sections, vary greatly in size, scope, and ability. Europe's policy-makers, industry, and users – the composers – draw on their knowledge of the strengths of various instruments to write a cohesive plan that elevates the product of the whole. The European Commission and individual member states act as the conductor, attempting to guide what could otherwise be a cacophonous rabble into a coordinated, mutually reinforcing harmony. Except, in the swiftly moving reality of tech policy, Europe is essentially attempting to write the music, construct the instruments, train the conductor and players, and perform the symphony simultaneously. The outcome does not yet resemble a stirring performance of Beethoven's Ode to Joy.

As a large, open economy, the EU remains highly reliant on outside actors – principally, the United States and East Asia – for its digital technology. On its current trajectory, the EU will remain a global tech player in the coming

---

---

decade, but will have less room for maneuver as it confronts a tougher, more competitive global tech landscape than has previously existed. As the battle for digital competitiveness heats up, the EU's success in advancing its capacity to act will be determined along the following dimensions which interact and inform each other:

- First, its regulatory power – the EU's ability to establish rules governing the development and use of technology at home and to effectively shape global tech governance in a way that advances Europe's objectives.
- Second, its innovation power – Europe's ability to both develop and, perhaps more importantly, commercially adopt new technologies to enhance Europe's global industrial competitiveness.
- Third, in many ways the linchpin for the first two, the EU's market power – the means by which the EU is able to instrumentalize access to its market and deepen unfettered activity within its market as a means of incentivizing conformity of non-European tech players with European rules. Harnessing European market power relies on a policy mix that combines both the EU's regulatory and industrial instruments.

Taken together, these dimensions form the basis with which the EU will shape its digital technology landscape as it heads toward 2030. This monitoring exercise examines past instruments and current ambitions.

---



# Three Scenarios for the Digital Environment in 2030

In the technology scenario workshop that was conducted in November 2020, participants examined key drivers affecting Europe's ICT landscape as it attempts to develop as a global tech leader. The workshop identified three possible scenarios for Europe's digital outlook in 2030. Of the three, the baseline scenario is the most likely outcome – both the best- and the worst-case scenarios are possible, but not necessarily probable. Ultimately, despite commonalities between the baseline and best-case scenarios, the baseline is surprisingly equidistant from the scenarios on either extreme. Each scenario is outlined below:

**The baseline scenario:**  
“Coding 2020 into 2030”

**The worst-case scenario:**  
“Made in China 2030”

**The best-case scenario:**  
“A Strong Europe in a Stable World”

In the **baseline scenario** – “Coding 2020 into 2030” – continued US political oscillation between populism and liberal internationalism forces the EU to pursue “contingent unilateralism.” The scope and level of adoption continues to grant the EU an ability to set global technology standards. The EU provides new rules on AI, cloud computing, industrial data, platforms, and competition that lay the ground rules for both Europe and non-EU third countries. As it does so, however, Europe suffers from innovation stagnation due to an increasingly securitized and fragmented strategic technology landscape in areas like data flows, ICT infrastructure, mergers and acquisitions (M&A), and tech investment. The fusion of engineering-driven manufacturing and user-driven smart devices puts Europe's home-turf prowess in automobiles, heavy machinery, and appliances in direct competition with a phalanx of dynamic upstarts from China and the United States (e.g., Tesla, Xiaomi, and

Haier). Attempts to provide state aid to startups and innovative divisions of legacy companies largely flounder under the weight of cumbersome bureaucracy and the risk-averse strategies of public authorities responsible for managing public investment. Unable to compete on quality and user experience with new US and Chinese players, but still maintaining a large market with access predicated on playing by EU rules, Europe consolidates its role as rule maker and tech taker. The EU clings to its role as the tech referee, setting regulations on data and competition globally – perhaps adding new regulatory areas like AI and cloud – even as it continues to lose ground in innovation.

## BOX 1 – BASIC DEFINITION OF THE TECH STACK:

There are four general layers in the “tech stack,” or the parts of the digital ecosystem. Broadly defined, they are:

- The physical layer (e.g., cables, telecommunications infrastructure like 5G equipment, and physical computational infrastructure like semiconductors and IoT);
- The logical layer (e.g., internet Protocols, authentication, and packets and data);
- The platform layer (e.g., cloud and edge services, application programming interfaces (APIs), and other cross-cutting, platform-based offerings); and
- The application layer (e.g., discreet applications such as over-the-top (OTT) services like social media, streaming, instant messaging, and audio communication services).

No layer is clearly defined – each informs and permeates the others. Software and AI bind the layers together. Data flows through all layers.

In the **worst-case scenario – “Made in China 2030”** – the EU gradually becomes dependent on the Chinese technology stack (BOX 1). China's technological leadership slowly increases as Europe's predominant reliance on US tech gradually gives way to a reliance on China, starting with hardware, smartphones, and apps. This trend is reinforced by increasing European accommodation of the Belt and Road Initiative (BRI), which places China at the center of standard-setting efforts on issues of state-centric tech governance, cybersecurity, and technical standards. The gradual march toward dependency on Chinese technology is solidified with conditions buried in terms of service that lock in Chinese control over technological infrastructure associated with digital services. Access and control to this ICT infrastructure becomes privileged. China's preponderant control of technological services in Europe allows China to wield it as a political weapon. The EU loses its capacity to act as it must acquiesce to China.

In the **best-case scenario – “A Strong Europe in A Stable World”** – the EU becomes a full-fledged technological peer with the United States and China with equivalent essential patents, unicorns, venture capital, and IT talent. The three powers cooperate, sharing the benefits of emerging technologies. Intra-EU digital inequality – between countries as well as in the urban-rural divide – virtually disappears as access to 5G and online infrastructure is available to all, enabling strong EU sectors (e.g., IoT, robotics, health, mobility, and gaming) to thrive. The EU repeats the General Data Protection Regulation's (GDPR) success with Gaia-X, creating a federated cloud system based on European values that – becomes a global gold standard. This allows for global industrial and sectoral data pools. The pace of innovation in quantum, encryption, and AI is matched by robust, trustworthy regulation and education that shapes a competitive workforce, ensures carbon neutrality, and fosters citizen trust in new technologies.

Based on the best-case scenario, there are ten conditions that Europe would have to meet in order to optimize its technological capacity to act in technology – i.e., position Europe as a global tech leader (BOX 2).

The workshop demonstrated that concerns about technological dependency and the geopolitical implications of the tech race are of great concern. Simply put, in the context of the emerging US-China tech race, Europe's incumbent regulatory strength will likely be insufficient to achieve its desired role as a technological actor on par with the United States and China. Europe must couple its role as a regulator with new efforts to create an environment in which

indigenous innovation can flourish. Both the baseline and worst-case scenario reflected a loss of agency for Europe. Issues of significant political concern – such as technology's role in carbon emission mitigation, the advancement of a human-centric values system, and the promotion of digital equity in the Global South – became secondary in those scenarios as others placed more emphasis on control of technology itself.

### BOX 2 – CONDITIONS FOR EUROPE'S EFFORTS TO ACHIEVE GLOBAL TECH LEADER STATUS

- Complete the Digital Single Market with seamless digital services and regulations across the 27 member states;
- Guarantee supply-chain access and resilience at all layers of the technology stack;
- Establish leadership and control of critical and emerging technology areas;
- Develop deep, interoperable, easily accessible data pools;
- Unlock state, institutional, and venture capital (VC) investment;
- Attract global ICT talent;
- Conduct and commercialize emerging technology R&D;
- Broaden global regulatory and standard-setting leadership beyond personal data and competition;
- Strengthen cybersecurity in critical infrastructure and along all lines of digital operations; and
- Advance reliable tech alliances with like-minded states.



# Measuring the EU's Capacity to Act Across Five Benchmarks

This study explores the EU's capacity to act in digital technology across five categories: 1) how the EU defines the problem it is attempting to address; 2) how the EU sets an agenda; 3) how the EU formulates policy; 4) how the EU implements policy; and 5) to what degree European policy has an impact at home and globally. In each of these, it draws on the interactions, mutual reinforcements, and, at times, tensions between European power as a digital regulator, and its aspirations as a tech industrial leader at each stage of the policymaking process. Because digital tech policy is extremely heterodox, it is difficult to fit the policy making process neatly into these five broadly defined categories. This, in and of itself, is a limitation that the EU must confront and one that is explored in detail as part of this analysis. That said, this study works within the limitations of these categories and draws out some findings that could better position the EU to adapt to accelerating developments in digital technology in a geopolitical context.

## PROBLEM DEFINITION

Like other areas assessed in this exercise, the European Commission – along with key member states – is, on its face, skillful in its ability to define the problems it faces in digital technology. It is able to identify deficiencies and frame them. Commission President von der Leyen has made digital leadership one of the two main priorities, along with a green transition, of her strategy at the Commission. She has stated her belief that “Europe must have [the capability] to make its own choices, based on its own values, respecting its own rules,”<sup>1</sup> while also correctly lamenting that, in reality, “Europe is still punching well below its weight.”<sup>2</sup>

The sense of existential foreboding in the race for technological leadership is also underscored by member states, particularly the larger ones. France and Germany recently laid out Europe's 2030 ICT outlook in even starker terms, saying “the choice is simple when it comes to industrial policy: unite our forces or allow our industrial base and capacity to gradually disappear.”<sup>3</sup>

In examining the landscape, six key drivers emerge at the outset of Europe's “digital decade.” Each has been identified repeatedly by the European Commission. The following pulls together the most-identified themes, such as:

- **Europe's fragmented Digital Market:** Europe lacks the large, unified digital market operating with one language, legal culture, and capital market that makes the United States and China attractive for digital innovation. Europe's digital services market remains fragmented, lacking natural advantages in areas like cohesive language, culture, online behavior, and investment preferences.
- **The changing nature of technological development itself:** Access and control over platforms, cloud, internet infrastructure, advanced algorithms like AI, quantum technology, and advanced microprocessing are becoming central to economic, strategic, and democratic power and vulnerability. The level of adoption and sophistication of general-purpose technologies increasingly “provides the key value addition to” classical products and services. Legacy sectors like automotives, appliances, machinery, the industrial fabrication of chemicals, and pharmaceuticals – the heart of European industry – are increasingly based on software and data-processing. As such, Europe's legacy companies face fierce competition with US and Chinese tech competitors. The play for technological leadership is increasingly made on industrial turf, which Europe had long dominated.
- **The prospect of technological decoupling:** China's techno-authoritarian rise has bumped up against a United States increasingly willing to leverage global dependence on US tech for geopolitical aims. The resulting demand to pick a side, be it on semiconductor usage, data localization and access requirements, or even the protocols governing the future internet, is

1 Ursula von der Leyen, “Shaping Europe's digital future,” European Commission, February 19, 2020: <<https://t1p.de/i000>> (accessed March 11, 2021).

2 Ursula von der Leyen, “Keynote speech by President von der Leyen at the ‘Masters of Digital 2021’ event,” European Commission, February 4, 2021: <<https://t1p.de/t9kg>> (accessed March 11, 2021).

3 Bundesministerium für Wirtschaft und Energie and Le ministère de l'Économie, des Finances, “A Franco-German Manifesto for a European industrial policy fit for the 21st Century,” February 19, 2019: <<https://t1p.de/2luh>> (accessed March 11, 2021).

forcing Europe to quickly choose whether it will accept dual systems of ICT architecture, attempt to carve out an interoperable position that preserves access to both, or develop a third alternative. A complete split in two would encompass all aspects of the technological stack: the physical, protocol, platform, and application layers of the digital economy, as well as the algorithms and data they run on.

- The COVID-19-fuelled acceleration of Europe's digital dependences on external actors and consolidated Big Tech dominance:** Even before the COVID-19 crisis, the European Commission had defined its interest in revisiting its dependence on the United States and China. But the pivot to digital adoption fueled by the COVID-19 pandemic's economic and technological shocks drew Europe's existing technological dependency into high relief. Reliance on US platform services, from video conferencing to streaming services, combined with greater awareness of supply chain vulnerabilities in areas like semiconductors, created new urgency for Europe's pursuit of indigenous technological capabilities. Moreover, the dominance of Big Tech platforms has increased their ability to gatekeep everything from APIs used in contract-tracing apps to e-commerce, adtech, and cloud. The Commission's 2019 EU-China Strategy – which identified China as a “negotiating partner, economic competitor and systemic rival” – specifically emphasized achieving a “more balanced and reciprocal economic relationship.”<sup>4</sup> However, China's six-percent GDP growth in Q4 2020 amid pandemic conditions has accelerated the EU's market dependency on the Middle Kingdom, causing new reliance on Chinese IT as a condition for access to the Chinese market for European IoT applications like connected cars.
- The rise of state-backed industrial policy:** China's relative success in moving up the technological value chain in the last ten years has been a disruptive force in the global technology ecosystem. The Chinese Communist Party (CCP) has worked to fuse state and enterprise together. This unified structure can take different forms, from fully state-owned enterprises to theoretically independent enterprises like Chinese Big Tech with party-heavy management boards. This sort of vertical system incorporates massive state-run national and local investment and procurement structures that give preference to state-favored companies,

forced joint ventures, and shared technology intellectual property (IP) gathered through state-backed industrial espionage with copy-cat companies at home. The codependence with the state, with the CCP as the undisputed senior partner, is a hallmark of China's domestic technology sector, and its presence has become a benchmark of its expansion in areas like telecommunications hardware, handsets, fintech, e-commerce, social media, and IoT. The fusion has driven other large powers, notably the United States, but also the UK, Canada, Japan, South Korea, and the EU, to revisit how they support access to and control key technologies.

- Weakening models for digital governance:** The desire to create parallel governance structures, contested global standards, and attempts to claw back control from international, multistakeholder governance bodies are affecting the global nature of the internet itself. Overall, repeated, disparate attempts to repatriate digital governance by countries like China and Russia are threatening a balkanization of the digital space. In China, these include the Huawei-led effort to establish a next-generation network and protocol system known as “New IP”; sweeping data localization requirements written into the 2017 Internet Security Law that mandate “important data” be stored in-country, which could impact European access to industrial data; and increasing use of antitrust law to rein in control of private Chinese Big Tech actors like Alibaba. In India, 2021 revisions to the national law governing intermediaries require new content moderation and grievance redress infrastructure based in-country, adding to existing and increasingly stringent data and supply chain localization requirements.<sup>5</sup>

Each of these six trends – reflected in the baseline scenario and taken to their extremes in the worst-case scenario – are clear and present in the minds of Brussels' most senior policy makers. As a strategic matter, the Commission has long identified digital market fragmentation as a source of both economic and geopolitical weakness of Europe. However, the key external drivers above have caused Europe to reassess beyond strictly market terms. The European Union and its member states have identified broad outcomes necessary to address these policy challenges. Generally, the EU has attempted to shape a digital technology environment in which:

<sup>4</sup> European Commission, “EU-China – A strategic outlook,” March 12, 2019, p. 6: <<https://t1p.de/39fz>> (accessed March 11, 2021).

<sup>5</sup> “New Rules For Online News And Social Media: 10-Point Guide,” NDTV, February 25, 2021: <<https://t1p.de/f0vw>> (accessed March 11, 2021).

1. High quality, safe connectivity is accessible to all EU citizens;
2. ICT processes – particularly the processing, transfer, and storage of data – is accessible through data spaces and consistent with Europeans' fundamental rights;
3. Rules governing digital services and data usage are uniformly enforced;
4. The Digital Single Market across Europe is pursued;
5. European actors are increasingly competitive;
6. Europe has control over key technologies and access to secure, resilient supply chains;
7. Europe has indigenous, reliable digital infrastructure; and
8. Sustainability and the green transition are linked to digitalization goals.

The European Commission and leading member states are capable of accurately contextualizing and diagnosing Europe's deficiencies in a global context. There is no complacency trap when Brussels compares Europe's innovation industrial base with peer competitors. The European Union has worked to create instruments to strengthen control of strategic technology development and tech transfer. New instruments have been specifically developed with technology projects that draw on EU R&D funding (e.g., Horizon Europe) or strategic technology (e.g., suppliers to the Galileo satellite network). The goal behind these instruments is to broaden the EU's tech industrial base. Sovereignty in technological matters can only be ensured if the EU itself is capable of developing and producing relevant technology, an area in which it has fallen far behind the United States and is losing ground to China. The EU and its member states have identified this problem and are focusing on key aspects, most importantly bolstering its capabilities in semiconductors<sup>6</sup> and quantum computers,<sup>7</sup> as well as focusing attention on internet infrastructure.<sup>8</sup>

However, the EU has difficulty defining the problem and setting up a framework in three interrelated areas. First, given the scope of the defined challenges, Europe at times finds itself unable – or unwilling – to prioritize often conflicting objectives. This is not new. Even in its landmark policy achievement, the General Data Protection Regulation (GDPR), assessments of the EU's policy approach are not

unanimous. On the one hand, the EU is proud of its creation of the global standard for personal data. On the other hand, the EU sees where it might have been a victim of its own success – creating a standard that ties its hands when faced with competitors in the US and Asia able to use personal data more freely. Europe's conflicting objectives have also spilled over into the way the bloc views data storage infrastructure location, and ownership. Europe's European Data Protection Supervisor (EDPS), France's Commission nationale de l'informatique (CNIL), and Germany's Federal Data Protection Act (DPA) have all expressed reservations about both data transfer to the United States and the use of US cloud service providers based in Europe. They base their reservations on legal access requirements for law enforcement and intelligence services.

Second, the EU still has significant blind spots in providing frank, clear-eyed assessments of the real trade-offs of its digital policies. For instance, first-mover regulations contributed to the bloc's paucity of data and, as a result of this and other factors (e.g., fragmented markets, risk culture, capital access, research commercialization), Europe missed out on the first wave of internet innovation. As a result, the EU was less able to compete with the United States and China as a globally competitive social media and e-commerce actor. While Commission officials and others rightly claim that the GDPR has "become a model for large parts of the world," they are less willing to acknowledge the costs associated with it<sup>9</sup>, from a more difficult regulatory environment for tech startups to an inability to provide sophisticated data analytics that could accelerate vaccine distribution in the COVID-19 pandemic.<sup>10</sup>

Third, senior political leadership in the EU can find itself bound by regulators, the former pursuing high strategic stakes, the latter asserting narrow legal norms. Independent Data Protection Agencies (DPAs), whose independence is protected by law, have a narrow focus on GDPR enforcement, with other objectives – like innovation, sustainability, tech adoption – falling outside their mandate. DPAs and the European Court of Justice (ECJ) set a high bar for GDPR enforcement and limited the Commission's ability to maneuver. For instance, on multiple occasions, the Commission has negotiated data flow agreements with the United States

6 European Commission, "Member States join forces for a European initiative on processors and semiconductor technologies," December 7, 2020: <<https://t1p.de/90e90>> (accessed March 11, 2021).

7 Deutsche Bundesregierung, "Bund fördert Quantentechnologien" [The federal government promotes quantum technology], January 15, 2021: <<https://t1p.de/xw58>> (accessed March 11, 2021).

8 Laurens Cerulus, "Lisbon eyes undersea cable investment to bolster EU tech infrastructure," Politico, December 10, 2020: <<https://t1p.de/hqwe>> (accessed March 11, 2021).

9 Ursula von der Leyen, "Open letter from the President of the European Commission, Ursula von der Leyen, to Mathias Döpfner, CEO of Axel Springer SE," European Commission (January 29, 2021): <<https://t1p.de/5m8xm>> (accessed March 11, 2021).

10 Hannah Balfour, "Could GDPR be impeding the global COVID-19 pandemic response?," European Pharmaceutical Review (October 2, 2020): <<https://t1p.de/2ukf>> (accessed March 11, 2021).

that were later invalidated by the European Court of Justice (ECJ) because they did not meet GDPR criteria.<sup>11</sup>

## CAPACITY TO DEFINE THE PROBLEM



The EU is able to successfully identify challenges to its ability to achieve global leadership status as a technological rule-maker and innovator. However, it lacks the ability to successfully prioritize its challenges; often has a blind spot for challenges of its own creation; and fosters strategic gaps between institutional actors.

## AGENDA-SETTING

In broad terms, the EU is an active and, at times, ambitious agenda-setter. The European Union has long centered digital policy at the core of its work and devoted resources and effort to articulating its agenda. EU action often reflects dominant contemporary political narratives and rising technologies, with the agenda recently shifting from a market to a geopolitical orientation. The Commission has, at several junctures, framed its digital agenda in the context of broader strategic narratives. The EU has the ability to synthesize disparate member state and institutional interests into broad strategies reflective of technological trends and the geopolitical environment. In recent discourse, two stand out as the EU has moved from a narrative around the Digital Single Market to digital sovereignty.

In the context of awareness of the deficiencies in Europe's ICT landscape, the Commission formulated the 2015 Digital Single Market Strategy, launched by then-Commission Vice President Andrus Ansip, which aimed to assemble Europe's fragmented market landscape into a unitary space for consumers, businesses, start-ups, civil society, and regulators. The DSM centered around three interlocking elements: 1) seeking to promote access, 2) increasing fairness and innovation, and 3) encouraging economic growth. Its primary mode of action was removing internal market barriers and delivering visible user benefits, a plan meant to promote cross-border commercial activity in digital services. At the

time, EU innovation czar Robert Madelin summed up the DSM's guiding logic stating, "the most important thing 'Europe' creates is not the law but the space."<sup>12</sup> The DSM included a number of legislative measures aimed at knitting the EU closer together, for instance eliminating geo-blocking, allowing greater cross-border portability of online content, and easing e-commerce parcel delivery. This effort was championed by multiple Council presidencies, with the 2017 Estonian EU Council Presidency deeming the free movement of data the "5th freedom" alongside the free movement of goods, services, capital, and people.<sup>13</sup>

As the transatlantic triple shocks of Snowden, Trump, and Cambridge Analytica entered Europe's policy bloodstream, discourse – particularly in Germany – increasingly focused on the framework of digital sovereignty. Its concept of sovereignty centered on the individual citizen and their ability to control the storage, transfer, and processing of personal data as a fundamental right. However, implicitly, it also addressed cybersecurity and access denial to snoops like the NSA, and carried with it strong potential data localization effects.

By 2015, it grew to encompass a broader innovation industrial base. The current German definition of digital sovereignty is based around three principles:

1. A market landscape that allows for competition and the development of new business models independent of dominant players;
2. Access to trustworthy technology adhering to strong regulations; and
3. Framework conditions at the German and European levels that allow for high standards for data sovereignty.<sup>14</sup>

This definition reflects the ordoliberal traditions of innovation and industrial development in Germany, albeit with a harder geopolitical edge. And it was reaffirmed by German Chancellor Angela Merkel at the November 2019 Internet Governance Forum: "In my understanding, digital sovereignty does not mean protectionism or the dictates of government agencies as to what information can be disseminated, but rather describes the ability to shape the digital transformation in a self-determined manner, whether as an individual, a single person, or as a society."<sup>15</sup> In some

11 In the 2015 Schrems I and 2020 Schrems II decisions, the court invalidated the commission's findings in light of PRISM mass surveillance programs revealed by Edward Snowden.

12 Carl Bildt, Building a Transatlantic Digital Marketplace: Twenty Steps Toward 2020 (see note 7), p.19.

13 Council of the European Union, "EU to ban data localisation restrictions as ambassadors approve deal on free flow of data," June 29, 2018: <<https://t1p.de/708o>> (accessed March 11, 2021).

14 Nadine Brockmann, "Digitale Souveränität im Fokus von BMWi und BITKOM," Basecamp, May 22, 2015: <<https://t1p.de/8kpu>> (accessed March 11, 2021).

15 Erste Lesung, "German EU Council Presidency: Digital Sovereignty" (October 20, 2020): <<https://t1p.de/2ml9b>> (accessed March 11, 2021).



ways, the regulation- and market-building DSM agenda and the industrial policy-centered “digital sovereignty” agenda were a complimentary division of labor between the EU and its largest member state.

At the same time, the French have consistently urged Europe to adopt a notion of digital sovereignty centered on innovation, industrial build-up, and control of data within European territory. This desire reflects a long tradition of interventionist, state-centric industrial policy in France. The German and French notions cohabitate in a sort of strategic ambiguity, currently under active negotiation with each other as digital sovereignty takes form in projects like Gaia-X and others working toward the development of greater semiconductor production capacity.

The Commission's greater geopolitical emphasis, President von der Leyen's leadership, and the COVID-19 crisis combined to spark a deep rethink of the EU's position on technological access and control. This has fueled the accurate perception that digital single market creation is not enough, a recognition that has become a through line in EU agenda-setting.<sup>16</sup> Across the board, from Macron to Merkel, and from the Commission to the European Parliament (EP), Europe is defining its quest for digital sovereignty as a “third European way of digitization which contrasts with the US-American and Chinese approach.”<sup>17</sup> Supply shortages in medical goods and semiconductors, and increased demand for remote work during the recent COVID-19 crisis, have led to an even stronger emphasis on industrial shortcomings within the EU. Now, digital sovereignty is largely seen to include all aspects of technology, especially the digital infrastructure needed to both communicate, generate and process data.

Generally, Europe's approach to digital sovereignty lacks the defined objectives and outcomes that characterized the DSM Strategy. The drawbacks are clear. But it also has advantages. The French commissioner for industry, digital rights groups, and German ordoliberalists can all embrace the term “digital sovereignty.” The strategic flexibility derived from this catch-all term gives actors in Europe – both the Commission and individual member states – the ability to take ownership and drive initiatives from the ground up.

This à-la-carte approach impacts agenda-setting with mixed, at times muddled results. For instance, when discussing digital sovereignty achievements during its 2020 Council Presidency, Germany emphasized industrial policies on in cloud computing, quantum computing, semi-conductors/micro-processors, digital identities, and data governance. The German Presidency also allowed major new legislative proposals on issues including platforms and the market dominance of online gatekeepers, which remain in the purview of the Commission, and areas like the digital services tax, where Germany remains principally ambivalent.

In the past, the clear accent – reinforced in the 2000 Lisbon Agenda – was on economic competitiveness and innovation. As the EU moves toward 2030, that emphasis has expanded to include components addressing access and control of key technologies. Already in February 2019, France and Germany issued a 14-point Franco-German Manifesto for a European Industrial Policy Fit for the 21st Century.<sup>18</sup> In it, France and Germany began to outline specific areas: massive industrial investment, changes to Europe's regulatory framework, and new measures to protect Europe's industrial base. The document pointed favorably to new policy developments around Important Projects of Common European Interest (IPCEI) that allow for greater deployment of state aid in microelectronics, questioned the impact of competition policy that could prevent the emergence of European tech champions, and advocated more active screening of investment, public procurement access, and trade policy to ensure consistency with strategic autonomy and an evolving definition of digital sovereignty. In December 2020, 18 EU telecommunication ministers signed a joint letter stating that Europe needs the capacity to “design and eventually fabricate the next generation of trusted, low-power processors, for applications in high-speed connectivity, automated vehicles, aerospace and defense, health and agri food, artificial intelligence, data-centres, integrated photonics, supercomputing and quantum computing.”<sup>19</sup> Other IPCEIs are in the works on network infrastructure equipment, cloud computing, hydrogen power, and batteries.

The Biden administration also sparked a reset of European agenda-setting around tech policy. More strident calls to wall off digital dependences have paused in some corners of the Commission and select member states as both attempt

16 “While a strong single market, open competition and trade policy are critical assets for the EU's economic success and resilience, a massive scale-up of investments is also necessary.” See: European Commission, “Roadmap: Communication on a Europe's digital decade: 2030 digital targets” (February 10, 2021), p. 2: <<https://t1p.de/ij0j>> (accessed March 11, 2021).

17 Julia Pohle, “Digital sovereignty A new key concept of digital policy in Germany and Europe,” Konrad Adenauer Stiftung (2020): <<https://t1p.de/sqz4>> (accessed March 11, 2021).

18 Less than two weeks after the commission blocked the Alstom-Siemens Rail merger.

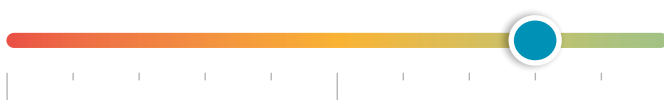
19 European Commission, “Joint Declaration on Processor and Semiconductor Technologies,” December 7, 2020, p. 3: <<https://t1p.de/ur9w>> (accessed March 11, 2021).



to synchronize the EU's digital regulatory, standard-setting and market access agenda with renewed EU-US cooperation in the Trade and Technology Council. Diverging views on these issues could give rise to new intra-European tensions, with Germany and smaller northern European states on one side and France on the other, and elements of the Commission divided between both camps.<sup>20</sup>

What is nevertheless clear is that, in contrast to the DSM – which included specific targets largely related to market standardization and liberalization – Europe's quest for digital sovereignty places greater emphasis on the EU and member states taking a more interventionist role in shaping the digital environment. Through the post-COVID-19 Next-GenerationEU recovery plan, IPCEIs, and national industrial policy, that focus is in four areas: 1) public investment in connectivity; 2) a stronger industrial and technological role in strategic areas of the digital supply chain; 3) building a “real data economy” as the engine for job and value creation in Europe; and 4) a business environment that encourages competition against the backdrop of dominant US tech players, particularly in light of accelerated technological adoption due to pandemic-related lockdowns.<sup>21</sup> Even efforts to create a uniform single market environment in areas like neutral data brokerage and the responsibilities of gatekeepers by and large raise regulatory conditions and call for greater state intervention rather than liberalizing conditions.

## CAPACITY TO SET THE AGENDA



The EU is able to craft an agenda that is flexible and responsive to what it perceives as key challenges. It can synthesize perspectives, particularly those of large member states, into a broad policy narrative, often taking advantage of strategic ambiguities that mask differences between key actors.

## POLICY FORMULATION

Europe's digital tech policy formulation is ambitious and heavily informed by geopolitical circumstances. Questions remain, however, as to how the EU can translate its objectives into effective action and to what extent it can enlist

like-minded democracies in its efforts. Two broad dimensions characterize Europe's efforts to develop policy to shape its technological environment. First, Europe's recognition that the global ICT landscape does not reflect its values. In addressing this, the EU is making an aggressive bid to bring its market power to bear to rewrite the world's digital rulebook. The European Union is in the midst of reinforcing its role as a digital technology regulator through a set of policy initiatives clustered around core legislation on digital platforms and data services – namely, the Digital Services Act (DSA), Digital Markets Act (DMA), Data Governance Act (DGA), and AI Regulation and Data Act. Additionally, the EU is developing softer law elements that deal with media pluralism and disinformation, data governance, artificial intelligence, cloud computing, and cyber. This also encompasses Europe's ability to shape the norms and standards environment, an area of priority as Europe aims to put itself in the position to “set standards, rather than follow those of others.”

Second, Europe perceives deficits in the control of critical and emerging technologies and has accordingly begun to raise its industrial policy profile in response. These efforts include classical industry support in the form of direct state investment, increased R&D, efforts to encourage open standards in areas where European players lack incumbent status, and investments in human capital – much of it funded through the 2021 post-pandemic Recovery and Resilience Fund (RFF), a “€620 billion” bazooka for which 20 percent of member state investment must go to digitization. Increasingly, the Commission is also working with member states to sharpen market access tools like export controls, enhanced investment screening, academic openness, and strategic use (and exemptions) from competition rules, all in order to shape its digital technology environment.<sup>22</sup>

European tech policy transmission is structurally diffuse given structural and philosophical frictions within the European Union. It is also characterized by multilevel governance where regional public sector actors and private players often lead.

Much of this is intentionally designed, reflecting the decentralized, interdisciplinary nature of tech policy in Europe. Even at the Commission level, responsibilities are divided throughout the organization with multiple commissioners and directorates-general holding lead competencies.<sup>23</sup> The Commission has, however, struggled with this fragmented

20 Angela Merkel et al., Letter to Ursula von der Leyen (March 1, 2021): <<https://t1p.de/wdxk>> (accessed March 11, 2021).

21 European Commission, “Europe's moment: Repair and Prepare for the Next Generation,” May 27, 2020: <<https://t1p.de/5dsc>> (accessed March 11, 2021).

22 European Commission, “A Europe fit for the digital age”: <<https://t1p.de/lq0i>> (accessed March 11, 2021).

23 These include DG CONNECT, DG JUST, DG COMP, DG GROW, DG HOME, DG MOVE, and DG TRADE. Additionally, regulatory bodies across data protection (the European

policy transmission landscape. In 2019, the incoming Commission attempted to streamline tech policy by placing it in the hands of Margarethe Vestager, the coordinating executive vice president for a “Europe fit for the Digital Age,” but many of the core tech competencies – data protection, digital trade, disinformation, and cybersecurity – remain outside her institutional purview. As a result, policy formulation often reflected long, deliberative processes and subsequent compromises, a reality that often leads to contradictory policy objectives. Moreover, other public institutions have constrained the Commission’s ability to use competition authority to advance a level playing field for tech actors operating in Europe.<sup>24</sup> Many cases have raised questions about the Commission’s ability to authoritatively negotiate with key partners. For example, the EU-US Privacy Shield agreement on the free flow of personal data across the Atlantic and its predecessor, the Safe Harbor Framework, were both struck down on the basis of how the European Court of Justice interpretes fundamental rights and subsequent rulings by member state Data Protection Authorities (DPAs). These interpretations leave out the key role that European member state intelligence communities play, for example, in bulk data collection, and EU member state intelligence services are not a part of data agreement negotiations with third countries.

This fragmented policy structure is reflected at the member state and subnational levels as well. In Germany, policy formulation is scattered across ministries and agencies. This has led to conflicting priorities and outlooks based largely on different institutional cultures. For instance, recent debates around certification procedures for trusted 5G equipment providers in Germany’s IT-Sicherheitsgesetz 2.0 have pitted the Defense Ministry, the Federal Foreign Office, and the Interior Ministry on the one hand against the Economic Ministry, Chancellery, and Federal Office for Information Security (BSI) on the other. In the absence of a head of government with a clearly defined point of view, this kind of diffuse distribution of power makes strategic coherence in tech policy difficult.

The Commission recognizes difficulties in coordinating consistency. DG Connect has been designated a coordinating hub for the EU’s February 2020 Digital Strategy and was given the task of “analysing global market and technology developments [and] providing geostrategic perspec-

tives.”<sup>25</sup> This is a useful innovation to link implementation of Europe’s digital ambitions with the need to anticipate both technological and international changes. Moreover, it is directly linked to the RFF allocation process. The Commission also maintains the DSM Strategic Group, a body coordinated by DG Connect that meets three times annually to incorporate member states, non-member states, and the Commission in a process that tests and refines ideas and definitions, and provides a sounding board and opportunity to establish buy-in for pending policy initiatives. The group does not, however, incorporate non-state actors or have a mandate to evaluate previous initiatives.

But these bodies can lack sufficient political weight to address difficult tradeoffs, the ranking of priorities, the ranking of priorities, and those assessments necessary to create a consistent through line in tech policy that bridges objectives in critical areas. Agendas are broadly set by Germany, France, and the commission. While this can lead to necessary policy breakthroughs, the diffuse power centers can also create long policy formation delays and reflect Byzantine processes meant to satisfy conflicting stakeholders.<sup>26</sup>

### CAPACITY FOR POLICY FORMULATION



The EU’s decentralized distribution of policymaking in digital technology combined with the lack of a strong executive creates difficulties and inconsistencies in policy formulation.

Data Protection Supervisor/Broad), telecommunications (BEREC), technical standards (CEN-CENELEC), and cybersecurity (Enisa).

24 Javier Espinoza et al, “Apple wins landmark court battle with EU over € 14.3bn of tax payments,” Financial Times, July 15, 2020: <<https://t1p.de/8zbzc>> (accessed March 11, 2021).

25 European Commission, “Coordination of Digital Strategy and Green ICT (Unit F.1)”: <<https://ec.europa.eu/digital-single-market/en/content/coordination-digital-strategy-and-green-ict-unit-f1>> (accessed March 11, 2021).

26 European Commission, “Digital Single Market Strategic Group (DSM SG),” March 7, 2019: <<https://ec.europa.eu/digital-single-market/en/strategic-group-digital-single-market>> (accessed March 11, 2021).

## POLICY IMPLEMENTATION

Europe is entering into a new phase in its efforts to implement its ambitious technology policy agenda. It is premature to judge its success. But in general policy implementation, several trends and limitations are worth noting.

### Steady Regulatory Centralization and its Limitations

Brussels, backed by some member states, has long attempted to draw tech regulatory policy toward itself. The Commission's latest policy push is tied to a clear impulse to centralize enforcement authority in Brussels. All of the cornerstone tech legislative proposals – the Digital Services Act, Digital Markets Act, Data Governance Act, and AI rules – are regulations. Each sees a greater role for the Commission in enforcement, with the DSA draft going the furthest and making the Commission the ultimate regulator on content moderation. It is unclear whether this power centralization will make it through the negotiating process unscathed, but the intent is clear: establish greater enforcement consistency by making the Commission the central authority at the expense of national regulators.

The logic is rooted in the Commission's responsibility for the functioning of the internal market (Art. 114, TFEU). Overall, the Commission's aim is to move steadily toward a more uniform regulatory environment for platforms and industrial data, to match its efforts on personal data with GDPR. There is pushback, however. Some larger states are already looking to claw back Commission-centered authority in new draft proposals. The true zenith of tech regulatory centralization was perhaps reached when the Commission rolled out its regulatory proposals; but the moment could be fleeting – the European Council has already moved to pick it apart. Nevertheless, the steady move toward digital regulatory frameworks is marked by a stealth centralization toward the Commission combined with federated oversight board structures like the European Data Protection Board.

The process of implementing policy can be arduous. For example, lifting roaming charges took ten years to implement and still contains a number of carve outs around areas such as data usage. The draft ePrivacy Regulation is a prime example of the EU's occasional inability to simply conclude matters in a timely fashion.<sup>27</sup> Caught in the push-and-pull, the regulation's ultimate passage has been delayed by more than two years and is only inching slowly forward.<sup>28</sup> But long

implementation lags can create uncertainty and ultimately impact the degree to which the regulation ends up being fit for its purpose, given continual technological development.

### The Rate of Technological Adoption vs. Rate of Regulatory Adoption

The pace of regulatory progress lags behind an ever-accelerating technology development product cycle, impacting the ability to future-proof policy. Technological developments in facial recognition, biometrics, IoT, and autonomous decision making are outpacing the policy environment addressed in the GDPR, which itself took six years to enact, from the first draft legislation until its entry into force in 2018. Quantum computing will have a similar issue with encryption and cybersecurity rules. This is especially true as new technologies and use cases emerge. Consideration for platform regulation for the legislative proposals that ultimately became the DSA and DMA began as early as 2013 and have yet to be concluded. They will likely last at least two more years, as negotiations with the European Council and Parliament move through multiple iterations. Legislative proposals for artificial intelligence remain limited, despite multiple expert bodies at the EU (e.g., High Level Expert Group) and national (e.g., Bundestag AI Enquete Commission) levels. The dynamics of technological change demand that the EU revisit the rules environment for both personal – as new forms of AI-based processing and decision making come online – and non-personal data.

The EU is working to anticipate technological trends to properly shape its regulatory objectives. For instance, as data processing moves from centralized computing facilities to connected objects, it is looking toward data governance and cloud structures that can provide guardrails for technological change. Still, with the policy cycle lagging years behind the ICT product cycle, it is difficult to chart a regulatory trajectory that can anticipate emerging tech areas. As a result, policy implementation can – in some cases – unintentionally hamper the EU's competitiveness internationally, reduce its technological sovereignty, increase its dependence on external actors, and thus reduce the EU's capacity to act.

### Enforcement Arbitrage and Capacity

Even as the EU steadily accumulates control over many aspects of tech regulation, actual enforcement of regulations

<sup>27</sup> The draft ePrivacy regulation was meant to update the 2002 e-privacy directive (Directive 2002/58/EC), to address rules governing user privacy on electronic communications, specifically pertaining to browsers, cookies, and messaging apps.

<sup>28</sup> Philip Grill and Samuel Stolton, "Mixed emotions as Council finally adopts position on ePrivacy text," EURACTIV, February 11, 2021: <<https://t1p.de/78kt>> (accessed March 11, 2021).

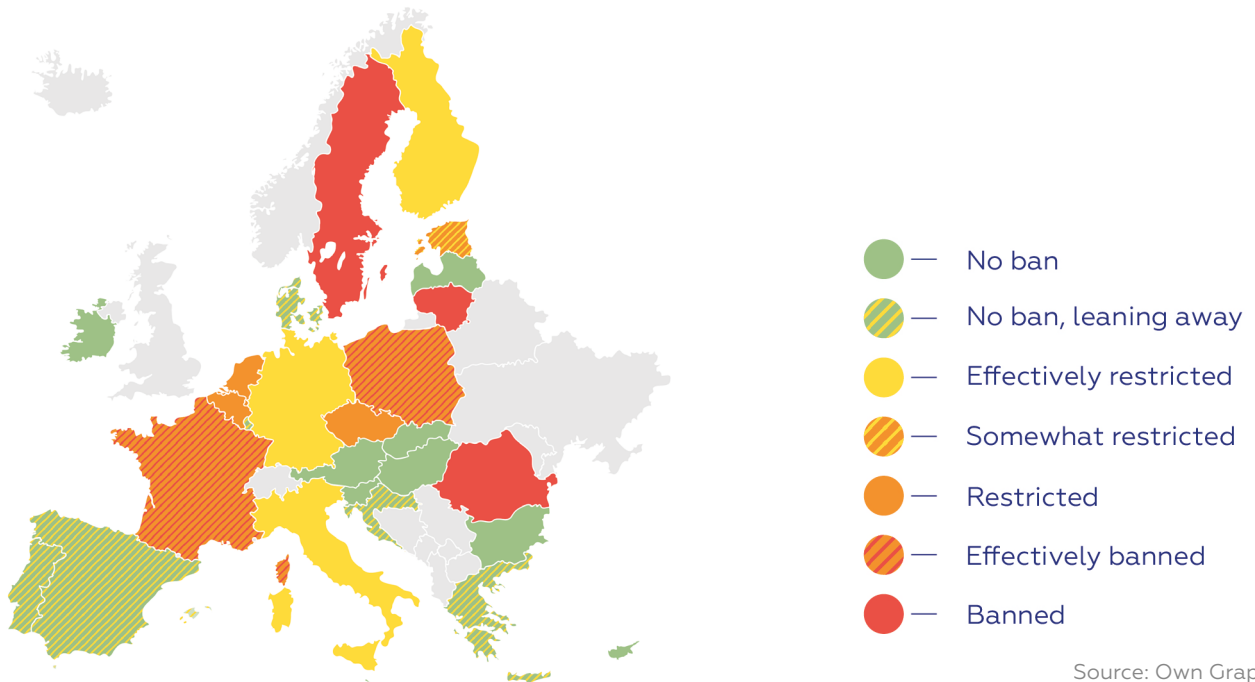
remains uneven across the bloc. In GDPR enforcement, for example, public Data Protection Authorities reflect the EU’s subsidiarity principle with decisions made at the national – and in Germany’s case, *Länder* – level. This has given rise to some degree of enforcement arbitrage, and data protection enforcement has thus been uneven across the EU. Big Tech players have shopped for favorable enforcement jurisdictions, with most landing on Ireland.<sup>29</sup> Ireland has worked to foster the most favorable environment to attract outside, non-European tech investment and has been accused of demonstrating some aspects of enforcement capture. Relatedly, compliance capacity can play a somewhat hidden role in unevenness across the EU. Take, for example, cyber incident reporting to national cyber authorities in accordance with national transpositions of the EU Network and Information Security (NIS) directive. The fact that the Netherlands and Germany have the highest level of cyber incident reporting is not an indicator of vulnerability. Quite the opposite – it demonstrates the degree to which the private sector feels legal and cultural pressure to observe breach notification requirements.

### The Limits of Coordinating Instruments

In areas where the Commission’s regulatory authority is limited, but a clear strategic interest exists in raising awareness and driving convergence, the EU has begun making more frequent use of coordinating mechanisms with a variety of policy instruments. But as the Commission itself acknowledges, “the still limited convergence across member states including a different pace of implementation of essential EU legislation” has hindered the EU’s ability to complete the Digital Single Market.<sup>30</sup>

In tech policy, two recent examples stand out. First, the 2020 5G Toolbox, developed under the auspices of the NIS Coordinating Group, established a set of uniform benchmarks which member states could use to assess cybersecurity risks in 5G networks based on a coordinated risk assessment report. As such, member states agreed to raise security requirements, diversify sourcing, and restrict risky supplier involvement (e.g., Huawei). It also flags potential Commission instruments – competition, trade, and certification – that can be used to support security.<sup>31</sup> Because 5G connectivity might increase IoT adoption, it is seen as in-

### Huawei Trusted Vendor Regime Status



Source: Own Graphic

29 The Irish Data Protection Commission (DPC) issued its first GDPR related fine in December 2020, more than two years after the law came into force. The fine, € 450K lodged against the social media platform, Twitter, has been criticized by other EU DPAs and privacy rights advocates. Natasha Lomas, “Twitter fined ~\$550K over a data breach in Ireland’s first major GDPR decision,” TechCrunch, December 15, 2020: <<https://t1p.de/xkt7>> (accessed March 11, 2021).

30 European Commission, “Communication on a Europe’s digital decade: 2030 digital targets,” 2021, p. 2: <<https://t1p.de/f1u>> (accessed March 11, 2021).

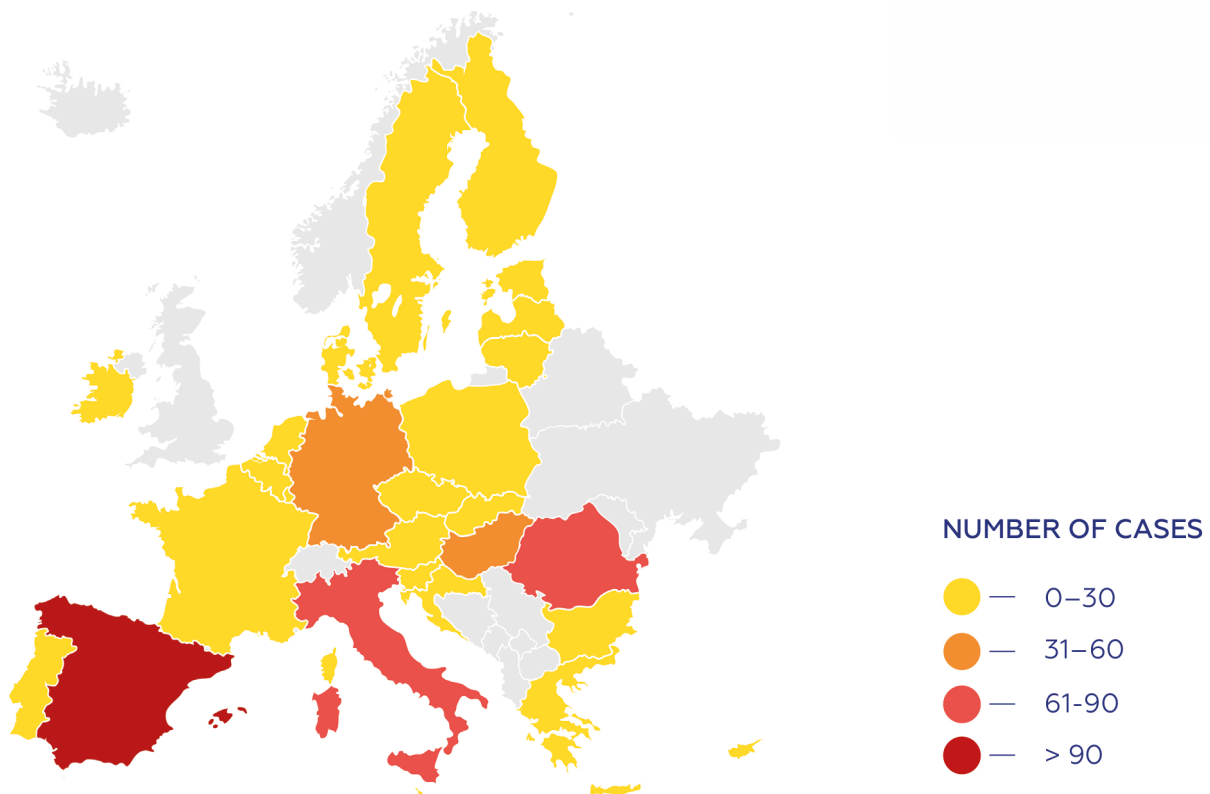
31 European Commission, “Secure 5G networks: Questions and Answers on the EU toolbox,” January 29, 2020: <<https://t1p.de/gccg>> (accessed March 11, 2021).

creasing the cross-border nature of telecommunications coverage. While there has been concern regarding 5G cyber risk, it is clear that this has not led to harmonization, as noted by the European Court of Auditors.<sup>32</sup>

Second, the EU’s mechanism for **investment screening** of inbound foreign direct investment (FDI) into projects of critical “European interest”<sup>33</sup> focuses on more institutionalized information-sharing, broad criteria that member states may draw on, and coordination between member states and the Commission. Germany, in anticipation of new guidelines, drafted amendments to its own screening mechanisms. They reflect a significant shift from previous strategic sector screening around raw materials and manufacturing to a preponderance of instruments targeting Germany’s tech sector – including its nascent startups in areas like health

AI. However, the tool has its limits. First, the EU has limited authority to uniformly define security interests – the willingness to block US tech investment, for instance, is under active discussion in some member states, while others see no threat. Ultimate decision-making power rests with individual member states, opening up the possibility of lateral vulnerabilities based on divergent risk perceptions. Second, member states lack a uniform sense of capacity – currently, eight member states have no form of investment screening at all.<sup>34</sup> Third, again, Europe is confronted with hard choices created by potentially conflicting objectives. Decisions to limit non-European investment into the start-up community, for example, could exclude potential US and Asian venture capital at a time when the paucity of risk-oriented capital is seen as a defining hurdle in Europe’s tech scene.

### Number of GDPR Enforcement Cases that have Included Penalties

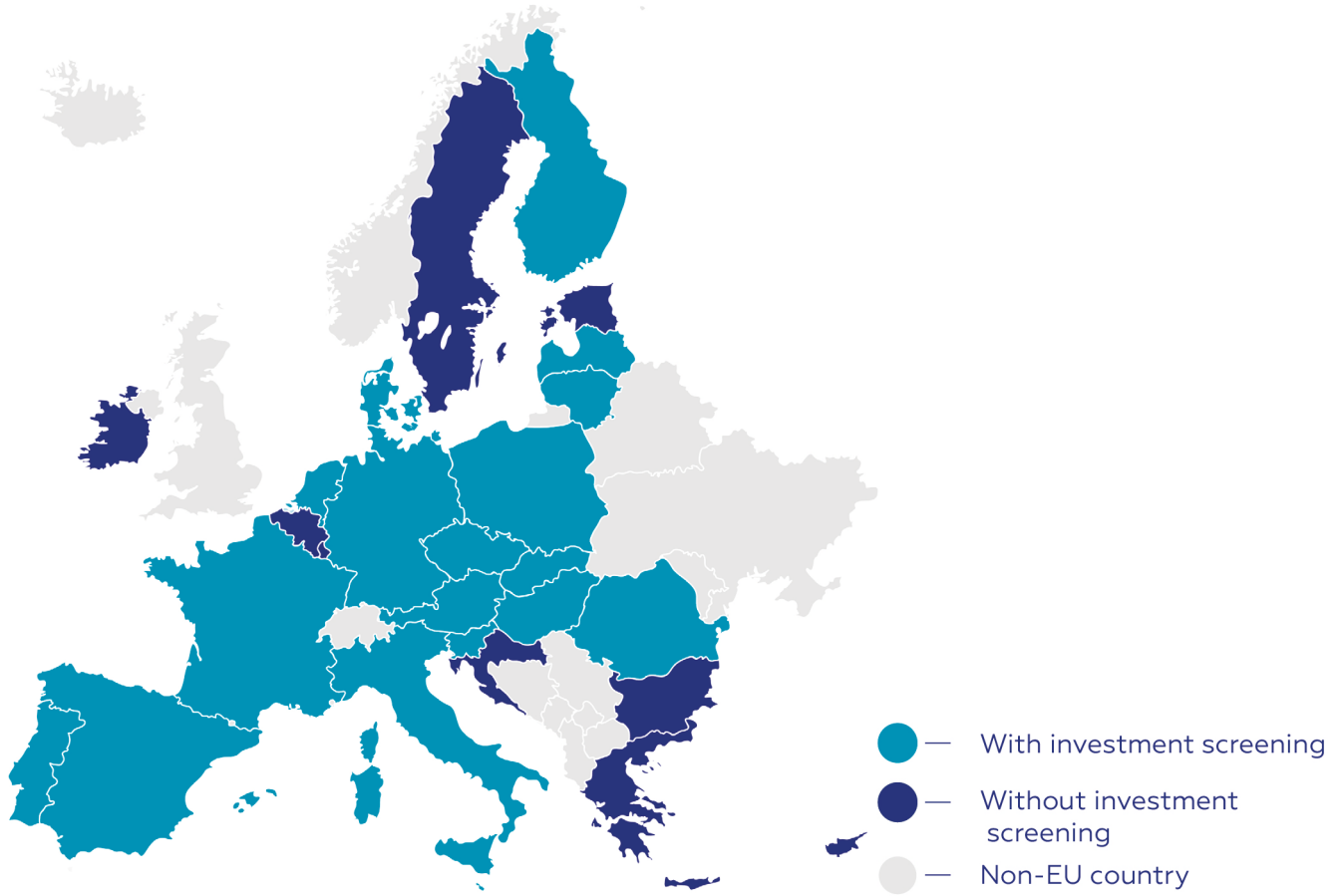


Source: CMS, “GDPR Enforcement Tracker,” 2021: <<https://www.enforcementtracker.com/>> (accessed November 19, 2021).

32 M. Apelblat, “EU auditors on 5G: Economic potential and security risks,” The Brussels Times, January 13, 2021: <<https://t1p.de/omo8>> (accessed March 11, 2021).  
33 European Commission, “EU foreign investment screening mechanism becomes fully operational,” October 9, 2020: <<https://t1p.de/q4st>> (accessed March 11, 2021).  
34 European Commission, “Secure 5G networks: Questions and Answers on the EU toolbox,” January 29, 2020: <<https://t1p.de/qccq>> (accessed March 11, 2021).



### Member States with Investment Screening Mechanisms Notified to the European Commission



Source: Own Graphic. Current states without Investment Screening Law: Ireland, Belgium, Luxembourg, Croatia, Estonia, Sweden, Bulgaria, Greece

#### A Latecomer to the National Security Dimensions of Technology Policy

Europe's most successful industrial projects like Airbus, Galileo, and the European Council for Nuclear Research (CERN) have recognized dual-use applications in certain technologies as geopolitical grounds for their indigenous development and control in Europe. That said, the shift toward digital regulation as the basis for European tech policy was largely coupled with a de-emphasis of the military implications that regulation could lead to. The EU continues to lack a means of assessing what its new rules on data governance, cloud, AI, and digital market power might mean for European military capacity.

With the movement toward greater state aid for the tech sector has come growing member state and Commission interest in integrated strategies that recognize the need for fact-based policy on ethical development and the usage of emerging, disruptive technologies in military contexts. The connective tissue between both the EU and allied civilian tech community and Europe's militaries is simply too weak given the strategic nature of general-purpose technologies. The EU has started to make a more concerted effort to bridge NATO, EU, and state emerging technology objectives, a policy area which extends beyond arms control and lethal autonomous weapons systems. This is particularly true in examining funding instruments like the 2021-27 Multiannual Financial Framework (MFF). The Commission's recent Action Plan on "synergies between civil, defense and space industries" is an impressive example of a new approach to

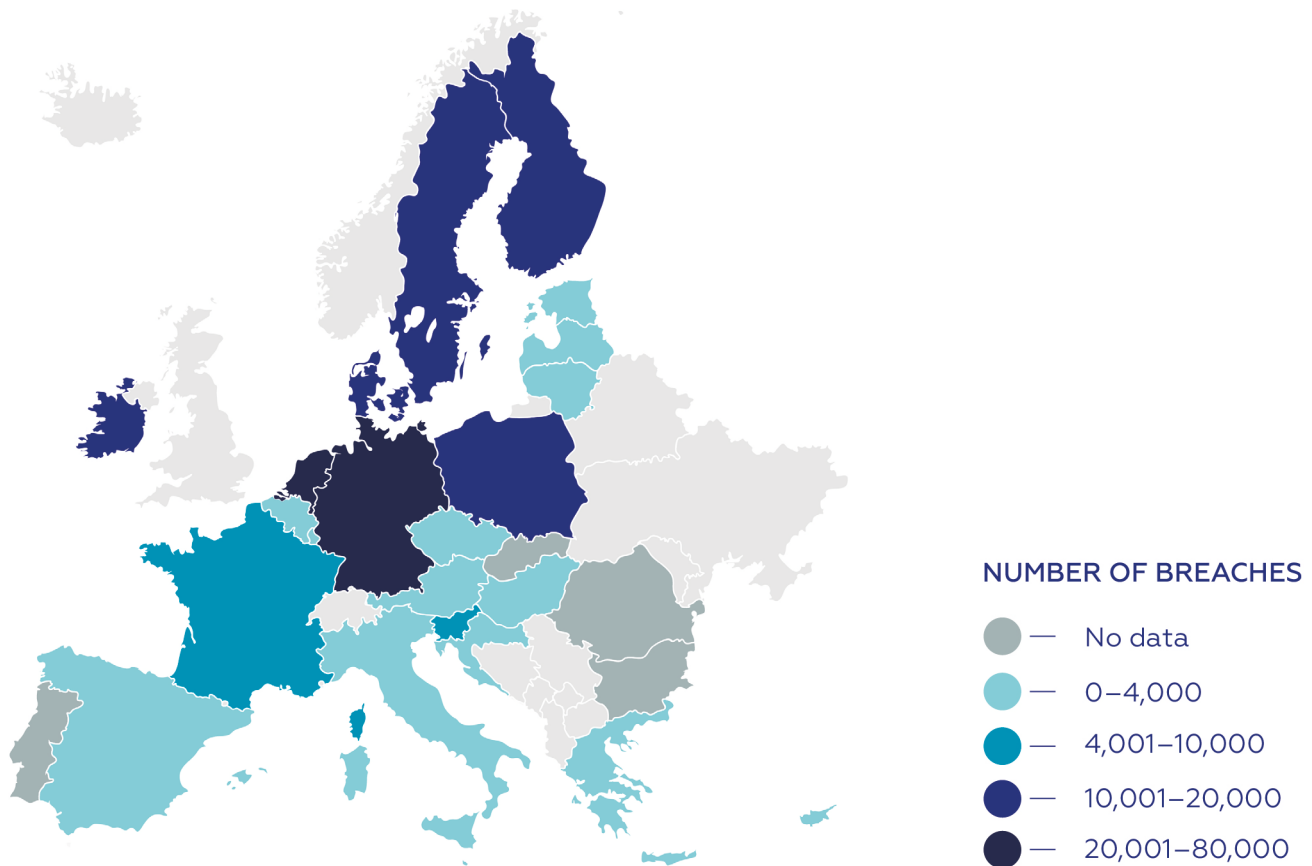
find cross-cutting complementarity in funding, recognizing spillovers between civilian and military research.<sup>35</sup> The Action Plan – which includes 11 actions and flagship projects in drone technology, secure space-based communication, and space traffic management – reinforces general aims outlined in the digital dimensions like more effective monitoring, operational standardization, and a recognition of the more general-purpose character of several emerging technologies. But incorporation of military applications into EU technology strategy and planning continues to be uneven – the 2021 Digital Compass, for instance, ignores the dual-use nature of key enabling technologies like cloud/edge computing, semiconductors, and quantum computing entirely.

### CAPACITY TO IMPLEMENT POLICY



The delicate process of moving the EU toward an “ever closer” digital and technology union hits limits in enforcement capacity, differences in compliance culture, and constraints on the mandate for the EU to enact policy. The mismatch between the pace of technological development and regulatory implementation also poses a challenge for the EU.

### Number of Company Breaches Affecting Personal Data Reported to State Authorities



Source: Joseph Johnson, “Number of personal data breaches in Europe 2018-2021, by country,” Statista, February 15, 2021: <<https://t1p.de/h5mz>> (accessed July 2021).

<sup>35</sup> European Commission, “Action Plan on synergies between civil, defence and space industries,” February 2, 2021: <<https://t1p.de/bbxw>> (accessed March 11, 2021).

## IMPACT CAPACITY

### The EU's Impact At Home

In 2030, Europe will be benchmarking its policy success on the basis of the 30 legislative proposals part of the Digital Single Market and a new slate of proposals in the current Digital Regulatory Package and post-pandemic Tech Industrial Policy. Assessing the impact of EU initiatives has traditionally been politically fraught. In the case of the Digital Single Market, the Commission largely failed to give a backend assessment of its overall market impact, one of the results of which has been that it has not always been confronted with hard truths of policy failures in acute terms. At the DSM's 2014 inception, the Commission estimated €250 billion in additional growth – including hundreds of thousands of jobs – by 2019 through its implementation.<sup>36</sup> However, the EU has yet to assess and review the program according to these standards. The outcomes are, at best, clearly mixed. But a clear assessment does not exist in any official capacity.

The Commission maintains a Digital Economy and Society Index (DESI) that provides a detailed mapping of enterprise tech adoption and usage across EU member states in five broad areas: 1) connectivity, 2) human capital, 3) use of internet services, 4) integration of digital technology, and 5) digital public services.<sup>37</sup> This gauge of member state performance is useful in examining the degree of convergence (or lack thereof) across the EU's Digital Single Market. However, it has largely steered clear of a critical analysis of the impact of EU tools and funding benchmarked to specific targets. Moreover, it does not define weaknesses and critical dependencies. In other words, while the DESI is a snapshot of internal trends of the Digital Single Market, it lacks a critical edge that would allow the EU to anticipate trends, pinpoint weaknesses in its own approach, and reflect the deeper geopolitical dimension of Europe's quest for digital sovereignty. Such a process is highly ambitious and resource-intensive.

In its October 2020 Council conclusions, member states asked the Commission to do just that. They asked the Commission to outline a Roadmap for the Digital Decade 2030 and present a comprehensive Digital Compass “which sets out the EU's concrete digital ambitions for 2030.”<sup>38</sup> The Digital Compass is meant to provide consistent monitoring of

EU digital targets and the key performance indicators currently lacking in the EU's digital benchmark, the DESI. It would standardize Europe's lines of effort – with targets and monitoring mechanisms – across a diverse set of digitalization policy areas ranging from industrial projects aimed at strengthening the EU's innovation industrial base to completing the DSM. Leaders have called for strong concrete targets (e.g., that all EU households should have gigabit internet, and all populated regions 5G coverage by 2030) and a monitoring process that is “permanent, recurrent and built on a wide societal, scientific and economic basis.”<sup>39</sup>

Given the qualitative differences in digital policy and highly differentiated resort responsibilities, both within EU institutions and at all levels of national, regional, and local government, a system of “transparent” benchmarks across portfolios and a monitoring process that accompanies the EU's public digital transformation effort – complete with a “traffic light” rating system – is long overdue. The EU set the stage for realistic and transparent benchmarking which should theoretically build on and cover gaps in the DESI. Like other efforts – including the European Semester for monitoring fiscal policy and the EU Strategic Compass for developing joint threat analysis and monitoring across crisis management, resilience, capability, and partnerships – a true assessment of success and failure in digital regulation and industrial policy would be highly political. Examining whether the Digital Compass is able to find its legs as an independent, objective, and credible assessment will be key to determining how EU policy improves Europe's technological capacity to act.

Some Digital Compass targets are extremely ambitious, particularly the effort to produce 20 percent of the world's high-end semiconductors in Europe by 2030. Other concrete targets are deceptively unambitious. Meeting many of these targets would not require any major course correction – conditions will essentially be met even if the EU follows a path between the baseline and worst-case scenarios in this forecasting exercise. For instance, the Digital Compass sets the goal of doubling the number of European tech unicorns – start-ups with a market value of over €1 billion – between 2021 and 2030. But between 2010 and 2020, the EU increased the number more than fivefold – from 10 to over 53.

<sup>36</sup> European Commission, “A Digital Single Market Strategy for Europe,” May 6, 2015: <<https://t1p.de/hj9n>> (accessed March 11, 2021).

<sup>37</sup> Each of these areas has a wide list of subsets that are dealt with including: 1) connectivity (e.g., broadband coverage, pricing, spectrum management approaches); 2) human capital (e.g., digital skills, ICT specialists, access barriers); 3) use of internet services (e.g., e-commerce, regular internet users); 4) integration of digital technology (e.g., digital intensity, cloud usage, cross-broader e-commerce); and 5) digital public services.

<sup>38</sup> European Council, “A digital future for Europe,” last reviewed May 6, 2021: <<https://t1p.de/lx7y>> (accessed July 20, 2021).

<sup>39</sup> Angela Merkel et al., Letter to Ursula von der Leyen (March 1, 2021): <<https://t1p.de/wdxk>> (accessed March 11, 2021).

### ASSESSING THE EU’S IMPACT AT HOME



The EU is improving its ability to assess the domestic impact of its digital agenda, complimenting the DESI with the Digital Compass and RFF monitoring. But blind spots around failures and at times unambitious targets continue to hinder effective impact assessments.

#### The EU’s Impact in the Outside World

The EU remains the world’s most important digital technology regulator. Leading the way as a “first mover” on data governance and strong competition enforcement culture, Europe has demonstrated the greatest influence on the data environment and tech market power both at home and abroad through its ability to regulate. Its capacity to shape algorithms has been less pronounced, partially because its role in regulating data has had upstream effects on its capacity to develop and commercialize cutting edge ICT based on algorithms, at least in the business-to-consumer (B2C) space that is poised to change through a series of new draft regulations.

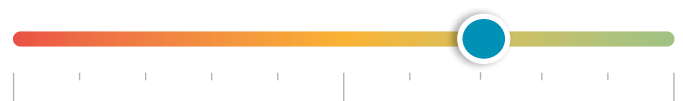
That regulatory strength is based on the threat of denying access to the EU’s 448 million citizens. It is also worth noting that the GDPR’s success comes as a function of the EU’s immense market size. Even as global tech companies have made the GDPR the lingua franca of data protection, the EU has racked up only a limited number of agreements with states to demonstrate that their data protection laws are “essentially equivalent” to that of the EU. This odd asymmetry is slowly dissipating as states like Argentina, South Korea, Japan, and Kenya, as well as subnational powers like California with the California Privacy Rights Act (CPRA), model data protection laws after the EU. However, it shows that the market access incentive for private companies is driving the GDPR’s role as a global standard – rather than the EU’s ability to bend states to its normative will. The same could also be the case on content moderation, cookie policies, and other aspects of data governance. The EU’s discourse on digital competition, market tipping, and network effects, as well as revisions related to content moderation, targeted advertising, and algorithm transparency are already having an impact on global discourse. The pending wave of EU regulation will provide a test case to monitor Europe’s ability project power on both private, non-European tech companies interested in market access as well as its ability to shape governance norms with non-European powers from California to China.

But the Brussels effect on tech is only as strong as the EU’s market power. In 2010, Europe’s share of the global economy was 21.5 percent, while the United States accounted for 23 percent. In the years since, the US economy boomed and Europe experienced uneven growth, but largely stood still. At the dawn of the 2020s, the United States had increased its relative share of the global economy, accounting for 25 percent, while Europe accounted for less than 17.5 percent. With the decline in its market relevance, the EU’s most important geopolitical asset – its market weight – is also diminishing.

Europe is overrepresented in technology norms coalitions, technical standard-setting bodies, and important, multi-stakeholder internet governance forums, and many of its member states are agenda-setters. For instance, France led in the creation of the Organisation for Economic Co-operation and Development’s (OECD) Global Partnership on AI and the Paris Call for Stability in Cyber Space. EU member states also consecutively chaired the last three internet Governance Forum (IGF) meetings, an important agenda-setting board. The EU has joined like-minded states, like the US, in past efforts to protect the multi-stakeholder system of internet governance.

By virtue of its technical expertise, financial resources, dynamic civil society, and large grouping of member states, Europe has, in the past, been able to saturate these bodies and largely shape global rules to reflect European values and be consistent with European standards. However, evident by the loss of relevance of the EU market vis-à-vis the United States, the EU has not been able to leverage this position to its advantage. Additionally, preponderant European representation has long been questioned and is increasingly coming under strain as states like China and Russia bid for technical standard-setting ecosystems. As a geostrategic corollary to China’s Digital Silk Road, Beijing is pushing for seats in standards-setting bodies and, in some cases, is creating new regional standard-setting bodies with itself as the hegemonic actor within these new arrangements.

### ASSESSING THE EU’S IMPACT IN THE WORLD



From GDPR to competition policy, the EU has proven itself a significant global tech rule maker. That capacity is a function of market size, however, and could diminish if not strengthened by innovation capacity.

---

# Germany's Role with Regard to the EU's Capacity to Act

Germany has been a driving force in Europe's efforts to shape its tech landscape. German nationals occupy key Commission roles associated with tech policy, German Members of the European Parliament (MEPs) often serve as rapporteurs on key digital regulation files, and German industry – telecommunications, automotive, and media in particular – have been skilfully aligning European tech regulation with their interests. Germany's ability to “flood the zone” in Brussels with tech policy personnel has had an immense normative impact on the trajectory of European digital tech policy.

First, Germany often effectively hoists an ordoliberal framework onto some of the EU's most important digital regulatory instruments. Prescriptive regulations like the GDPR are rooted in the notion that rules, particularly those based in German legal traditions, are best adept at setting digital market frameworks. German ordoliberal scepticism of market concentration and anti-competitive practices has also been a source of broad Commission mandates to aggressively address Big Tech market dominance. In these two areas, Germany is quite comfortable with EU-centered power. Both are correspondingly strong instruments and also strong projections of global regulatory power.

Second, Berlin systematically anticipates EU-level policy action, shapes its domestic legislation in advance of Brussels policy formulation, and thus creates reference conditions (and facts on the ground) for EU lawmakers. Europe's data protection philosophy – the basis for the GDPR – emerged in Germany in the 1980s before being hoisted on the EU. Germany's 2017 NetzDG played a key role in shaping the content moderation frameworks that fed into the Digital Services Act (DSA). Germany's 2015 IT Security Law intentionally interacted with, anticipated, and contributed to the ultimate framework for the NIS Directive. It replicated this anticipatory policy strategy in reforming the cyber law, the so-called IT-Sicherheitsgesetz 2.0, in anticipation of the 2021

NIS Directive reform. The 2017 German Datenethikkommission established a framework for assessing application and risk categories for artificial intelligence, a framework largely reflected in the EU's February 2020 AI White Paper, and the basis for the 2021 draft AI Act. Germany's 10th Amendment to the Act Against Restraints of Competition (GWB-Digitalisierungsgesetz) framed the debate on digital market power of dominant platforms, and Germany, together with France, provided legal architecture for the tipping classification for the Digital Markets Act.

Third, and perhaps most decisive for the 2030 period, is Germany's political influence on European industrial policy. Germany is traditionally more interested in Europe's regulatory ability than in its industrial policy ledger. However, Germany has grown somewhat comfortable with the pursuit of ICT industrial policy at the European level, historically the focus of the French government. As such, it has made significant movement in France's direction. In the February 2019 Franco-German Manifesto for a European Industrial Policy Fit for the 21st Century, France and Germany outline three specific areas: massive industrial investment, changes to Europe's regulatory framework, and new measures to protect Europe's industrial base.

But it remains unclear if Germany is truly ready to cross the industrial policy Rubicon at the European level. In the recent past, Germany has played a significant role in limiting, slowing, and even vetoing European tech policy ambitions. Germany's 2017-18 policy formation on artificial intelligence grappled with balancing regulatory and industrial policy aspects before ultimately deciding on an “AI Made In Germany” industrial strategy. The commitment to 20 percent of the Recovery and Resilience Facility (RRF) and the use of pooled funds remain controversial and, even though the coronavirus pandemic has spurred German backing for a large number of industrial policy initiatives, it is possible that Germany will course-correct after the crisis. Even within the German government, tensions appear to be emerging. Whereas the Economic Ministry (BMWi) has closed ranks behind an ambitious, EU-wide industrial vision for emerging disruptive technologies, serious doubts about a pooled EU industrial policy on emerging technology remain.

Across all areas, negotiating a logic for tech policy – “digital sovereignty” – will require efforts to bridge shades of difference between Germany, France, the Commission as well as other member states and constituents. More than anything, that could depend on how comfortable Berlin becomes with pursuing a Europe-wide technology industrial policy, something that Germany has historically been only half-heartedly committed or actively opposed to.

---



# Stocktaking: Assessment of Capacity to Act as a Whole

As the battle for digital technology competition heats up, the EU's success in advancing its capacity to act will be determined along the following dimensions:

- **Regulatory power** – the EU's ability to establish rules governing the development and use of technology at home and to effectively shape global tech governance in a way that advances Europe's objectives.
- **Innovation power** – Europe's ability to both develop and, perhaps more importantly, commercially harness new technologies as a source of Europe's global industrial competitiveness vis-à-vis peer competitors like the United States and China.
- **Market power** – the means by which the EU is able to instrumentalize access to its market and deepen unfettered access within its market as a means of bending non-European tech players to European rules and creating conditions to encourage cross-border digital services that support scalability and homegrown technology companies.

Brussels is experiencing a sense of existential distress about what technological changes mean for Europe's industrial base, external digital dependencies, and ultimately, its regulatory prowess. With an eye toward 2030, there is an acute awareness that the EU cannot "rest on regs." As the baseline and best-case scenarios indicate, the EU's regulatory position is a function of market size, a factor in relative decline. Its regulatory influence could slowly displace or break away

suddenly in what evolutionary theorists call punctuated equilibria.

The best-case 2030 scenario underscores that Europe's capacity to shape its digital environment is ultimately dependent on a benign international order in which states and other multi-stakeholder actors work cooperatively together to set rules. But in light of the rising tech conflict between democratic and authoritarian states, such an era of cooperation seems unlikely. As such, Europe's efforts must be predicated on the second-best operating environment: a confident, high-performing European digital economy embedded in an open, democratic, rules-based digital order. This need is particularly acute as the prospect of internet fragmentation, data localization, and greater instrumentalization of digital dependencies as political weapons become a more pressing possibility.

Given these likelihoods, the baseline and worst-case 2030 scenarios enter more clearly in the realm of the possible. The European Union is often able to identify its deficiencies and set an agenda both strategically – as it has done in the Digital Single Market and quest for digital sovereignty – and specifically – as it has done in DESI and recently updated through the Digital Compass and national RFF plans. On the regulatory side, the Commission is moving forward with its "Digital Package"<sup>40</sup> broadly centered on digital sovereignty in three areas: data governance, algorithms (particularly AI/machine learning), and platform regulation, as well as coordination on issues surrounding secure 5G infrastructure, investment, exports, and cybersecurity; and on the industrial side, toward new, post-pandemic IPCEIs in areas like semiconductors, edge computers, and batteries.

However, the EU's hydra-like structure in tech policy formation and implementation often prevents coherent, timely action, due to the diffuse distribution of competencies across Commission portfolios, DGs, national ministries, and often highly independent (and narrowly focused) regulators. Without a strong executive and given the trend toward more interventionist tech policy, the Commission and its member states must determine which actors have the big picture in mind and are capable of pursuing it with consistent, effective action.

Additionally, obstacles to completing the EU's Digital Single Market will always continue to be present. Language, consumer taste, culture, online behavior, taxation, and regis-

<sup>40</sup> First, the Digital Strategy outlined a plan to enforce "fair" use of platform dominance. Other areas touched on include content moderation, cloud infrastructure and cyber security. Second, the Data Strategy focused on creating nine sector-based data spaces allow data to flow freely across the EU, mandatory data sharing (including with governments) and includes GDPR reform proposals. It will include standardized forms of industrial data and IoT. Much of the strategy will be bundled in the Data Governance Act and draft Data Act in 2021. Third, the Artificial Intelligence White Paper addresses the regulatory environment for AI considering new testing standards for "trustworthy" AI in "high-risk" areas which is essentially anything that touches human lives.

tration models remain evident “non-tariff barriers to trade” in digital services. A glance at Europe’s fragmented e-commerce market – where big players like Amazon, eBay, and AliExpress dominate, followed by national champions (e.g., Otto and Real.de in Germany; Allegro in Poland; Bol.com in the Netherlands; Fnac and La Redoute in France) – demonstrates that limitations remain. In that way, the DSM will always be somewhat asymptotic – it will never cross the finish line.

In areas of Big Data pattern detection, machine learning, and AI, network effects are a key factor in creating the economies of scale necessary for cutting edge applications. In the race for data access, Big Tech – be it Chinese or American – has been able to establish competitive advantages at home which have allowed them an indigenous data well from which to draw when developing technologies. Moreover, they have been able to expand their offerings over time, increasingly

moving into new areas in media, artificial intelligence, smart home assistants, cloud infrastructure, and even internet cable infrastructure. The data access feedback loop is a function of market, capital access, talent availability, and regulatory environment which the EU has not been able to match.

Europe will not be able to achieve its capacity to act alone, and any conception of digital sovereignty that attempts to wall off Europe’s market to provide space for indigenous players to dominate is unlikely to succeed. An alternative approach would be building resilience through strong alliances based on strategic interdependencies, and policy choices that strengthen incumbent commitments to shared democratic norms and values. Joining forces with like-minded actors would provide Europe an opportunity to reduce its weaknesses and advance its capacity to act.

**IN SUMMARY:  
CAPACITY TO ACT  
ACROSS THE FIVE  
STAGES OF THE  
POLICY CYCLE**



Source: Author's compilation

# Implications and Recommendations Derived from the Monitoring Exercise

**Europe aspires to attain peer status both in innovation capability and rule-setting with the United States and China by 2030. Achieving this aim will not be easy. It will require sustained high-level engagement, investment, and hard choices. As an overarching goal, Europe should strive to address some of the policy cycle deficiencies identified in this study. They include the need to:**



**PROVIDE HONEST ASSESSMENTS OF PREVIOUS TECH INDUSTRIAL AND REGULATORY POLICY FAILURES, TRADE-OFFS, AND MEMBER STATE SHORTCOMINGS.**

The European Union should engage in an open stocktaking of successes and failures in past tech policy choices and initiatives. Confronting where and why state-backed projects like Euronet, Quero, DeMail, the Andromede cloud project, and others fell short will be essential for successful implementation of new IPCEI projects, Gaia-X, and RRF digitization initiatives. Even the GDPR, the EU's signature rule-making achievement, which has transformed global data protection, has confronted Europe with trade-offs and disadvantages that policymakers are often reluctant to acknowledge. This should include ex-post, ex-ante, and real-time iterative monitoring and benchmarking iterative monitoring and benchmarking processes that accompany

new projects and regulatory implementation in real time. The Digital Compass is a good start. It will be important for not only identifying laggards (as the DESI does), but also identifying why lags in implementation arise.



**FOCUS ON THE EU'S INCUMBENT TECH STRENGTHS IN SHAPING INNOVATION INDUSTRIAL POLICY.**

Europe has incumbent strengths in sensors, smart industrial machinery, B2B capabilities in areas like logistics, and robotics – strengths it should leverage to secure a more substantial production role in IoT. It should direct a combination of government-funded R&D, incentives for commercialization, and investment screening intended to keep and build out innovation capacity in Europe, especially in areas like artificial intelligence, quantum computing, cloud computing, and semiconductors. Europe must also continue to capitalize on its market, which solidifies its status as a dominant regulatory power and allows it to export European values through both its technology and rules.



**ALLOW FOR HARD-NOSED PRIORITIZATION IN SETTING STRATEGIC OBJECTIVES.**

A central tension at the heart of Europe's approach to digital policy is that tension between external competitiveness and internal cohesion. One can see it expressed in the AI White Paper, for example, which speaks of Europe as an aspiring "ecosystem of excellence" that leads in R&D, value chain development, and small and medium-sized enterprises (SME) competitiveness. On the other hand, it speaks of an "ecosystem of trust" which preserves and expands fundamental rights, consumer rights, and sustainability. The EU and its member states must be more capable of creating priority hierarchies in tech regulatory and industrial policy objectives. Setting effective and consistent policy remains tied to the ephemera of secondary and tertiary objectives like local economic development, untargeted R&D, politically difficult decisions about roles of non-European actors, sustainability, and social cohesion. This might require even greater tightening of portfolios falling under the digital tech policy umbrella within the Commission and a greater willingness of member states, particularly large ones, to elevate narrowly defined policy effectiveness above other objectives.



**EMBED EUROPE'S DIGITAL  
TECHNOLOGY STRATEGY MORE  
EXPLICITLY IN THE CONTEXT OF  
SIMULTANEOUS – AT TIMES  
COMPLEMENTARY – ACTION  
WITH LIKE-MINDED PARTNERS.**

Buoyed by the Biden Administration's entry into office, the EU has already embraced that trajectory: "The EU can only succeed in its digital transformation if it builds its Digital Decade in an outward looking manner.... [it] needs to strengthen its capacity to project its digital goals into its international cooperation promoting its human-centric, rules-based approach. This requires the development of partnerships and alliances that can underpin European investment in infrastructure, capacity building and the enabling environment, as well as fostering regulatory cooperation notably with like-minded partners."<sup>41</sup> The EU-U.S. Trade and Technology Council, in particular, will be an early test for Europe's ability to leverage its relationship with a like-minded power to shape both the global regulatory landscape and bolster its tech industrial resilience.

Europe must use the next ten years to close the existing gap in innovation, digital regulation, and tech industrial capacity to make it a trendsetter, a co-equal digital power with the United States and China. This vision of Europe as a trendsetter is ambitious, but achievable.

<sup>41</sup> Communication on Europe's Digital Decade: 2030 digital targets: "<https://t1p.de/miv7>" (accessed November 8, 2021)

---

# DGAP

Advancing foreign policy. Since 1955.

Rauchstraße 17/18  
10787 Berlin

Tel. +49 30 254231-0

info@dgap.org  
www.dgap.org  
@dgapev

The German Council on Foreign Relations (DGAP) is committed to fostering impactful foreign and security policy on a German and European level that promotes democracy, peace, and the rule of law. It is nonpartisan and nonprofit. The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the German Council on Foreign Relations (DGAP). DGAP receives funding from the German Federal Foreign Office based on a resolution of the German Bundestag.

**Publisher**

Deutsche Gesellschaft für  
Auswärtige Politik e.V.

**ISSN**

1866-9182

**Editor:**

John-Joseph Wilkins,  
Austin Davis

**Layout & Graphics**

Studio Friedrichter –  
Carl-Friedrich Richter

**Design Concept**

WeDo

**Photo of the Author**

© DGAP

**Cover Photo**

© ThisisEngineering  
RAEng / Unsplash



This work is licensed under a Creative Commons Attribution – NonCommercial – NoDerivatives 4.0 International License.

---