SITRA

WORKING PAPER

OCTOBER 2025

TECHNOLOGICAL CONVERGENCE

Pushing European innovation forward

Andrea G. Rodríguez
Director for Quantum Technologies, Adigital
Founder, The Policy Pulse

Fast-paced technological advances and growing geopolitical tensions are challenging Europe to rethink how it governs innovation. To enhance competitiveness, avoid technological dependencies and uphold its leadership in value-based digital development, Europe must invest in forward-looking governance frameworks at the intersections of critical digital technologies.

Sitra working paper

Technological convergence –
pushing European innovation forward

Author: Andrea G. Rodríguez
Sitra working group: Ella Palo, Laura Halenius, Krista Takkinen

Layout: Grano Oy

ISBN 978-952-347-424-6 (PDF) www.sitra.fi
ISSN 2737-1042 (online publication)

Sitra working papers provide multidisciplinary information about developments affecting societal change. Working papers are part of Sitra's future-oriented work conducted by means of forecasting, research, projects, experiments and education.

Contents

Foreword

Fast-paced technological advances and growing geopolitical tensions are challenging Europe to rethink how it governs innovation. To enhance competitiveness, avoid technological dependencies and uphold its leadership in value-based digital development, Europe must invest in forward-looking governance frameworks.

Critical digital technologies, such as quantum computing, artificial intelligence, semiconductors, and space technologies, are central to Europe's pursuit of strategic autonomy, competitiveness, and technological sovereignty. However, while advances in one field of technology frequently unlock new possibilities in another, current policy frameworks remain largely sectoral. This siloed approach risks slowing down innovation, fragmenting funding, and weakening Europe's ability to respond to emerging challenges.

This working paper by the Finnish Innovation Fund Sitra presents technological convergence as a tool for Europe to boost cross-sectoral innovation and strengthen its strategic autonomy. This paper has two key objectives. First, it introduces a working definition of technological convergence, examining the concept through European policy initiatives, technological maturity, and innovation structures and culture. Second, it provides tangible policy recommendations on how to govern technological convergence.

As the European Union prepares for its next budget cycle and reconsiders its innovation priorities, this working paper proposes embedding technological convergence into funding frameworks, impact assessments, and foresight processes. The paper frames technological convergence not as a future possibility, but as a present reality requiring active governance.

We extend our sincere thanks to **Andrea G. Rodríguez**, the author of this paper, for her valuable contribution. With the insights of this working paper, we invite you to join the conversation on how Europe can enhance innovation and growth by strengthening technological convergence.

Laura Halenius
Senior Lead, Sitra

Summary

This working paper addresses the concept of technological convergence as a strategic tool to enhance European innovation and resilience in the field of critical digital technologies. It introduces a working definition of technological convergence as the integration of previously isolated technology solutions developing into hybrid applications that unlock new capabilities and drive innovation.

The working paper analyses convergence from three perspectives. First, it provides an overview of European policy initiatives, tracing the evolution from strategic autonomy to sovereignty in digital governance. Second, it explores technological maturity and identifies convergence opportunities across the development, growth, and commercial phases. Finally, it identifies the innovation structures and culture that can facilitate convergence, highlighting the role of geopolitical and domestic factors in shaping innovation environments.

Technological convergence is further explored in practice through case studies of Physical AI, AI and cybersecurity, and semiconductors. These case studies illustrate how convergence is already shaping applications and value chains, though often without explicit policy support. The analysis shows that while convergence already takes place in practice, governance frameworks remain largely siloed, limiting the potential for scalable, cross-sectoral innovation at the intersections of technological fields.

To further drive European competitiveness through convergence, the working paper offers four policy recommendations:

1. Reduce fragmentation in funding schemes affecting critical digital technologies and establish clear research-to-market pathways.
2. Prioritise highly convergent technologies while using public funding.
3. Introduce technological convergence as a mandatory aspect in impact assessments.
4. Coordinate efforts to publish annual foresight reports on technological convergence in the EU.

The paper concludes that technological convergence is not a future possibility but a present reality, as innovation and growth are often found in hybrid technology solutions. Through foresight and strategic governance, technological convergence can provide grounds for more secure value chains and high-value hybrid applications, essential to building competitiveness and resilience in Europe.

Tiivistelmä

Tässä työpaperissa tarkastellaan, miten Euroopan innovaatiokyky ja resilienssi voivat vahvistua teknologisen konvergenssin avulla. Teknologinen konvergenssi tarkoittaa erillisten teknologisten ratkaisujen kehittymistä uusiksi sovelluksiksi, jotka mahdollistavat aiempaa useampien teknologisten hyötyjen yhdistämisen.

Työpaperi analysoi teknologisen konvergenssin käsitettä kolmesta näkökulmasta. Ensimmäisenä tarkastellaan, miten Euroopan komission politiikka-aloitteet strategisesta autonomiasta ovat vaikuttaneet digitaalisen hallinnon kehitykseen. Analyysi jatkuu teknologisen markkinakypsyyden käsittelyllä kehityksen, kasvun ja kaupallistumisen vaiheissa. Lopuksi tarkastellaan, miten eri alueiden, kuten EU:n, Yhdysvaltojen ja Kiinan innovaatiorakenteet ja -kulttuuri voivat vaikuttaa konvergenssin syntymiseen.

Teknologista konvergenssia tarkastellaan lisäksi konkreettisten tapausten kautta. Fyysisen tekoälyn (physical AI), tekoälyn ja kyberturvallisuuden ja puolijohteiden tarkasteleminen osoittaa, että teknologinen konvergenssi muokkaa jo nyt teknologisia sovelluksia ja arvoketjuja. Vaikka teknologiat yhdistyvät uusissa ratkaisuissa käytännössä, politiikkatoimet ovat edelleen suurelta osalta siiloutuneita. Tämä rajoittaa eri teknologiasektoreiden rajapinnoilla syntyvää innovaatiota.

Euroopan kilpailukyvyn edistämiseksi teknologisen konvergenssin avulla tämä muistio ehdottaa neljää politiikkasuositusta:

1. Vähennetään kriittisiin digitaalisiin teknologioihin kohdistuvien rahoitusohjelmien hajanaisuutta ja luodaan selkeä polku tutkimuksesta markkinoille.
2. Asetetaan konvergenssille potentiaaliset teknologiat etusijalle julkista rahoitusta käytettäessä.
3. Lisätään teknologinen konvergenssi pakolliseksi näkökulmaksi vaikutusten arvioinneissa.
4. Edistetään EU:n teknologisen konvergenssin vuosittaisten ennakointiraporttien julkaisua.

Työpaperissa todetaan, että tulevaisuuden innovaatio ja kasvu löytyvät usein hybriditeknologisista ratkaisuista, jotka hyödyntävät teknologista konvergenssia. Ennakoinnin ja strategisen ohjauksen avulla teknologinen konvergenssi voi tarjota perustan turvallisemmille arvoketjuille ja korkeaa lisäarvoa tuottaville hybridisovelluksille, jotka ovat olennaisia Euroopan kilpailukyvyn ja resilienssin rakentamisessa.

Sammanfattning

Denna publikation behandlar begreppet teknologisk konvergens som ett strategiskt verktyg för att stärka europeisk innovation och motståndskraft inom kritiska digitala teknologier. Den introducerar en arbetsdefinition av teknologisk konvergens som integrationen av tidigare isolerade teknologilösningartill hybrida applikationer som skapar ny kapacitet och driver innovation.

Publikationen analyserar konvergens ur tre perspektiv. Först och främst genom att ge en översikt över europeiska politiska initiativ och följa utvecklingen från strategisk autonomi till suveränitet inom digital styrning. För det andra genom att undersöka teknologisk mognad och identifiera konvergensmöjligheter i utvecklings-, tillväxt- och kommersialiseringsfaserna. Slutligen identifierar publikationen innovationsstrukturer och kultur som kan främja konvergens, med betoning på geopolitiska och inhemska faktorer som formar innovationsmiljöer.

Teknologisk konvergens utforskas vidare i praktiken genom fallstudier om fysisk AI, AI och cybersäkerhet, ochhalvledare. Dessa fallstudier visar hur konvergens redan formar applikationer och värdekedjor, ofta utan uttryckligt politiskt stöd. Analysen visar att även om konvergens redan sker i praktiken, förblir styrningsramarna till stor del uppdelade, vilket begränsar potentialen för skalbar, sektorsövergripande innovation i skärningspunkterna mellan teknologiska områden.

För att ytterligare främja europeisk konkurrenskraft genom konvergens föreslår publikationen fyra politiska rekommendationer:

1. Minska fragmenteringen i finansieringsprogram som påverkar kritiska digitala teknologier och etablera tydliga vägar från forskning till marknad.
2. Prioritera teknologier med hög konvergens vid användning av offentliga medel.
3. Införa teknologisk konvergens som ett obligatoriskt perspektiv i konsekvensbedömningar.
4. Samordna insatser för att årligen publicera framtidsrapporter om teknologisk konvergens inom EU.

Publikationen avslutar med att konstatera att teknologisk konvergens inte är en framtida möjlighet utan en aktuell verklighet, eftersom innovation och tillväxt ofta återfinns i hybrida teknologilösningar. Genom framtidsanalys och strategisk styrning kan teknologisk konvergens skapa en grund för säkrare värdekedjor och värdefulla hybrida applikationer, vilket är avgörande för att bygga konkurrenskraft och motståndskraft i Europa.

1. Introduction

Technology, understood as a driver of prosperity and geopolitical competition, has inevitably become the protagonist of numerous policy agendas. At a time where interconnectivity, once thought to lead to cooperation and peace, is increasingly weaponised for economic and geopolitical coercion, the development of forward-looking governance frameworks that better anticipate risks and promote innovation at the intersections of technologies has become crucial.

Recent events have underscored the vulnerabilities of the European technological agenda. Anticipating supply chain shocks and other disruptive events, such as the erosion of international institutions, and promoting cooperation in technology development and standards, is increasingly difficult.

As countries advance in the creation of strong policy frameworks that support long-term innovation, understanding technological convergence and its potential to amplify capabilities and accelerate innovation will be crucial in developing critical digital technologies. Examples of these technologies are advanced semiconductors, quantum technologies, advanced connectivity, cybersecurity solutions, and space and propulsion technologies.

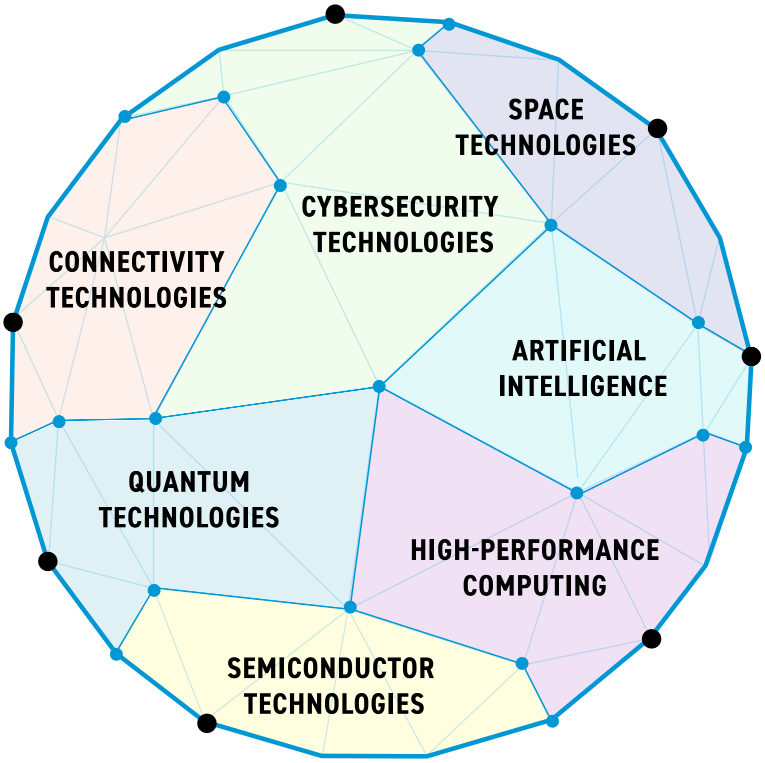
Technological convergence
is the condition in which previously isolated technologies converge, achieve a stage of stable growth, and can viably function and develop into new applications.

In an increasingly digitalised world, critical digital technologies are key to keeping industries and societies connected. Technologies such as artificial intelligence, semiconductors, quantum technologies, high-performance computing, 5G/6G networks, cybersecurity and space technologies form the backbone of innovation, changing industries, creating markets, and increasing the competitiveness of complex economies. These technologies, defined as the Critical Core (Figure 1, Technology Industries of Finland, 2025), are also blurring the boundaries between civil and military applications. As a result, countries are seeking not only access, but also control, with implications for areas such as scientific collaboration and international trade.

Understanding technological convergence is necessary for effectively governing innovation at the intersection of critical digital technologies. For instance, hardware-based technologies, such as quantum computing, will be fundamental to powering software-based technologies such as artificial intelligence. Similarly, the advanced data processing required to harness the full potential of 5G/6G networks will not be possible without AI models capable of managing the networks. At the foundation of it all lie computer chips.

Current policy and investment frameworks treat critical digital technologies as isolated clusters instead of networked technologies. They often fail to acknowledge the opportunities that arise when these are developed in coordination. Hybrid applications are the most probable drivers of economic and social transformation. Enforcing convergence in different technology fields can enable the construction of scalable architectures and enhance the efficient use of scarce resources, such as talent.

Figure 1: The Critical Core (Technology Industries of Finland, 2025)


SPACE TECHNOLOGIES
CYBERSECURITY TECHNOLOGIES
CONNECTIVITY TECHNOLOGIES
ARTIFICIAL INTELLIGENCE
QUANTUM TECHNOLOGIES
HIGH-PERFORMANCE COMPUTING
SEMICONDUCTOR TECHNOLOGIES

The Critical Core

At the core of these technological advancements lies data—its availability, quality, and security directly impact the effectiveness of AI models, the performance of high-performance computing (HPC) systems, and the reliability of quantum and secure communications. Europe's ability to process and utilise massive datasets, while at the same time ensuring data sovereignty, will be instrumental in enabling industries to fully harness the potential of interconnected digital technologies.

Connectivity, including 5G and future 6G networks, acts as a backbone for real-time AI applications, industrial automation, and secure digital infrastructure. Ultra-reliable, low-latency communications will accelerate edge AI, smart manufacturing, and autonomous systems, with direct implications for cybersecurity, quantum communications, and next-generation computing.

Quantum computing and communications hold the potential to revolutionise problem solving, encryption, and secure networks, benefiting from HPC, AI, and next-generation connectivity. Quantum computers, in synergy with AI, will address optimisation challenges in logistics, materials science, and drug discovery, while quantum-secured networks will redefine the security architecture of Europe's digital backbone.

Semiconductors are the foundation of all digital technologies, with their fabrication and supply chain playing a decisive role in ensuring technological sovereignty. Advances in semiconductor manufacturing will enhance AI efficiency, quantum-processing capabilities, and ultra-secure communication networks.

Cybersecurity serves as a cross-cutting enabler, safeguarding every layer of this interconnected ecosystem. AI-driven threat detection, quantum-resistant encryption, and secure-by-design semiconductor architectures will be crucial to ensuring Europe's digital resilience in an era of increasing cyber risks and geopolitical uncertainty.

Space technologies provide a critical infrastructure for global connectivity, earth observation, and AI-driven analytics. The fusion of AI with satellite imagery enhances climate monitoring, disaster response, and autonomous navigation, while space-based quantum encryption will play a key role in securing global communications.

Artificial intelligence (AI) relies on HPC and advanced semiconductors to process vast datasets, simulate complex models, and develop next-generation AI systems. Breakthroughs in AI architectures, such as neuromorphic computing, further drive the demand for specialised semiconductors and scalable computing power.

HPC fuels AI model training, quantum simulations, and secure communications, requiring cutting-edge semiconductor architectures optimised for massive computational workloads. As HPC infrastructure evolves, it enables faster AI-driven scientific discovery, financial modelling, and climate simulations, reinforcing Europe's technological edge.

2. Path to technological convergence

To drive strategic autonomy and competitiveness in critical technologies, Europe is seeking to create more robust value chains and globally competitive digital solutions. Technological convergence provides a policy framework to support innovation where it matters most – high-value hybrid applications.

Technological convergence is a new experimental approach to technology development and governance that fosters complementarity at the intersection of techniques, data and talent for the creation of hybrid solutions that are easier to scale and implement in the market.

Technological convergence can be understood as the condition in which previously isolated technologies converge, achieve a stage of stable growth and can viably function and develop into new applications. This concept draws inspiration from the well-established concept of "technology readiness level" (TRL), but takes it a step further by analysing implications around metrics such as degree of adoption, and substitution of previous technologies.

While nuances exist between different evaluation parties, TRL generally refers to the maturity level of a given product, from idea to market. However, as this study shows, TRL has its limits when it comes to defining the disruptive potential of a given technological application. This working definition argues that the state of convergence appears when two or more technologies develop in parallel but in a complementary manner, thus leading to the creation of technological products and applications that depend on the development of these separate technologies.

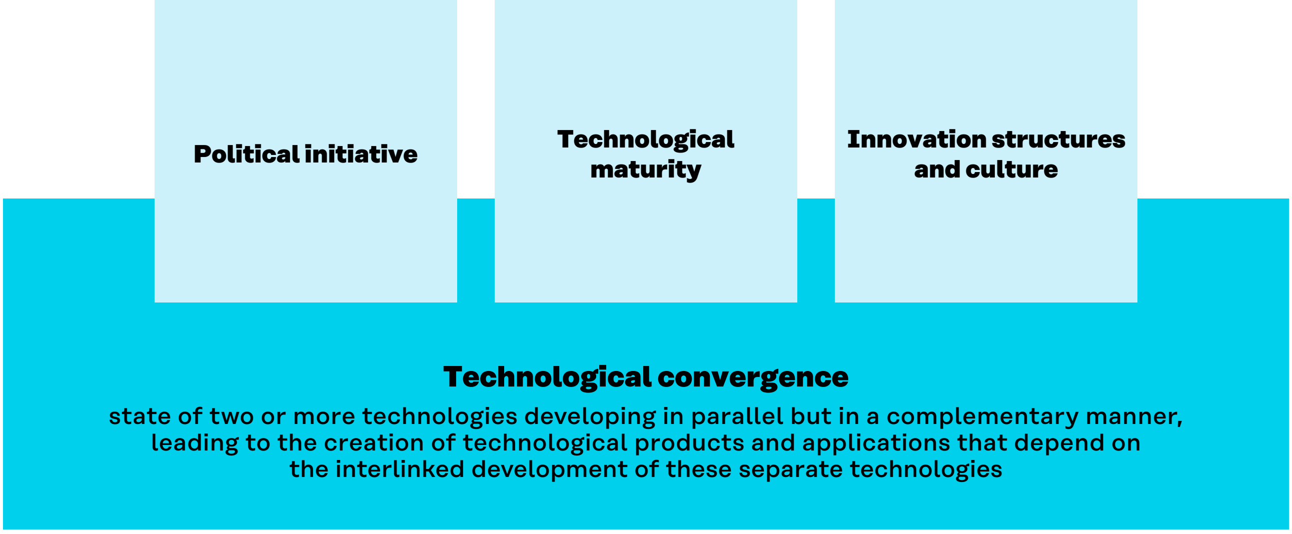
Beyond maturity, technological convergence is also the result of promising social, economic and political factors that facilitate experimentation at the interplay between different technologies. This innovation environment plays a significant role in enabling breakthroughs and shaping them into transformative applications.

As a recent report from the World Economic Forum (WEF) points out, when technologies combine, value chains converge and compound benefits emerge (World Economic Forum, 2025, pg. 7). Europe's strength in shaping markets through regulation must take a leap forward to foster technological convergence. Without understanding convergence between different critical technologies and value chains, the EU will struggle to effectively target measures to support its strategic autonomy.

Failure to govern convergence could result in new strategic vulnerabilities, such as technological lock-ins to non-European platforms, and the fragmentation of the internal market. Moreover, without addressing convergence, future action in EU digital policy will inevitably be siloed and reactive, unable to address compound risks or leverage cross-sectoral innovation. Europe's credibility as a global technological actor depends on whether it can treat the Critical Core not only as a

Without understanding convergence between different critical technologies and value chains, the EU will struggle to effectively target measures to support its strategic autonomy.

Figure 2. Enablers of technological convergence



state of two or more technologies developing in parallel but in a complementary manner, leading to the creation of technological products and applications that depend on the interlinked development of these separate technologies

collection of technologies but also as an integrated system.

Fostering this development requires an analysis of Europe's past and present initiatives aimed at strengthening strategic autonomy in the digital sphere. This chapter analyses the concept of technological convergence in the context of European Union from three perspectives: political initiatives, maturity, and innovation structures and culture.

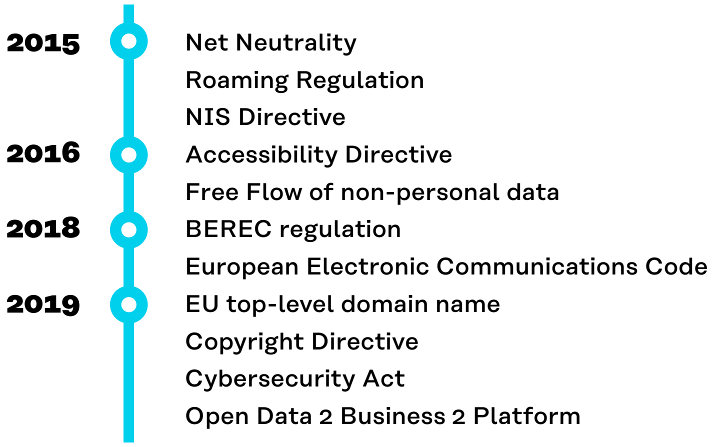
From resilience to strategic autonomy: technological convergence through European Commission initiatives

While technological convergence and critical digital technologies have only recently emerged as policy concepts, Europe's approach to technology governance has been deeply rooted in the concept of strategic autonomy. Analysing the development of strategic autonomy is essential for understanding the effects of technological convergence on the EU's current technology governance landscape. To effectively target future policy initiatives for enhancing innovation through convergence, a historical perspective on prior initiatives is necessary.

Over the past decade, the EU has made significant strides in recognising the strategic value of its single market, while at the same time acknowledging the negative consequences of openness. Since 2016, strategic autonomy has been related to the EU economy, democracy, and society. However, since the COVID-19 pandemic and the 2022 Russian invasion of Ukraine, the term has been extended to increasingly encompass security (Timmers, 2025).

In policy terms, "sovereignty" and "strategic autonomy" have been used interchangeably to invoke the ability of the EU to defend its own interests through the development of policies and partnerships. Nevertheless, a closer look at the term reveals that strategic autonomy can be defined in terms of capabilities, capacities and control (Timmers, 2024) to manage internal affairs. As Dr. Paul Timmers argues, fulfilling these three aspects requires a combination of

Figure 3. Overview of initiatives developed by the Juncker Commission.



internal and external measures. Increasing domestic capacities while establishing strategic partnerships enables the EU to act "multilaterally wherever [the EU] can, acting autonomously wherever [the EU] must" (European Commission, 2021).

Recently, reliable partnerships have been called into question, and interdependent value chains have revealed the vulnerabilities of a networked global economy. For instance, the COVID-19-induced semiconductor shortage affected major industries, such as the automotive industry, by the creation of supply bottlenecks that delayed manufacturing for weeks.

In contrast to the current political climate, strategic autonomy has not always been the defining feature of EU digital policy. It has rather been the consequence of a series of internal measures and external shocks that have given the EU the ability to act to protect common European interests instead of those of member states. This demonstration of "autonomy" has unfolded gradually over the last two European Commission terms.

The Juncker Commission (2014–2019): the end of laissez-faire policymaking on technology

The Juncker Commission was characterised by the consolidation of China as a global technology actor, Brexit, and growing concerns over online surveillance and the concentration of power in the hands of a few technology actors. These dynamics were fundamental in enabling the concept of strategic autonomy, initially rooted in the defence community, to start gaining ground in the realm of EU digital policy.

When Jean-Claude Juncker took office in late 2014, the EU economy had not yet fully recovered from the 2007–2008 financial crisis. Nonetheless, the EU's digital economy was showing promising growth, which helps explain the Juncker Commission's strong emphasis on developing the Digital Single Market.

The Digital Single Market Strategy (DSMS) (European Commission, 2015) outlined the EU's ambitions to create a well-integrated and digitalised environment for EU companies, while also introducing initiatives to reinforce consumer protection and digital rights. This particularly emphasised the right to privacy, which remained a pressing issue as the Snowden revelations were still looming in the background. Business-friendly, the DSMS brought about a number of successes, including roaming and net neutrality provisions.

During the Juncker era, the foundations were laid in digital policy sub-areas in which the EU would take a leading role, such as in cybersecurity (e.g. NIS Directive) and privacy protection (GDPR). Here, the focus progressively shifted from mitigating single market risks to addressing societal concerns. This change was partly driven by the UK's decision to leave the EU in 2016, with the Commission's quest to strengthen European unity amid rising euroscepticism (European Commission, 2017).

From 2017 onwards, the election of Donald Trump as president of the United States, coupled with the growing urgency to regulate the platform economy, combat data exploitation abuses, and reduce the concentration of digital infrastructure and resources in the hands of a few – largely controlled by American and Chinese firms – highlighted the EU's need to autonomously redefine its course, and acknowledge its innovation dependencies. By the end of the Juncker Commission, it had become clear that regulating the single market was more a political and geopolitical challenge than merely an economic one.

Moreover, during the Juncker term, China elevated its ambitions to become a technology powerhouse with the inauguration of the Made in China plan in 2015 (Government of China, 2015), which advanced measures to control critical digital industries, such as semiconductors, batteries, and artificial intelligence. In parallel to this, U.S. tech dominance, particularly in cloud computing, processors, and operating systems, led to a growing concern about the lack of EU players in strategic areas such as microchips, cloud infrastructure and battery manufacturing.

A wide range of measures were developed to mitigate these dependencies such as the 2018 Important Project of Common European Interest (IPCEI) on microelectronics and the launch of the European Battery Alliance (EBA), which sought to halt and reverse the EU's weakened technological position in the face of Asia's, particularly China's, production and supply monopoly on the lithium-ion batteries needed for Electric Vehicles (EV). This is a rapidly growing industry due to climate change concerns. Batteries were, at the time, a glaring example illustrating Europe's dangerous strategic dependence: despite being the second-largest EV market, its domestic battery manufacturing capacity remained minimal (McKinsey & Company, 2020).

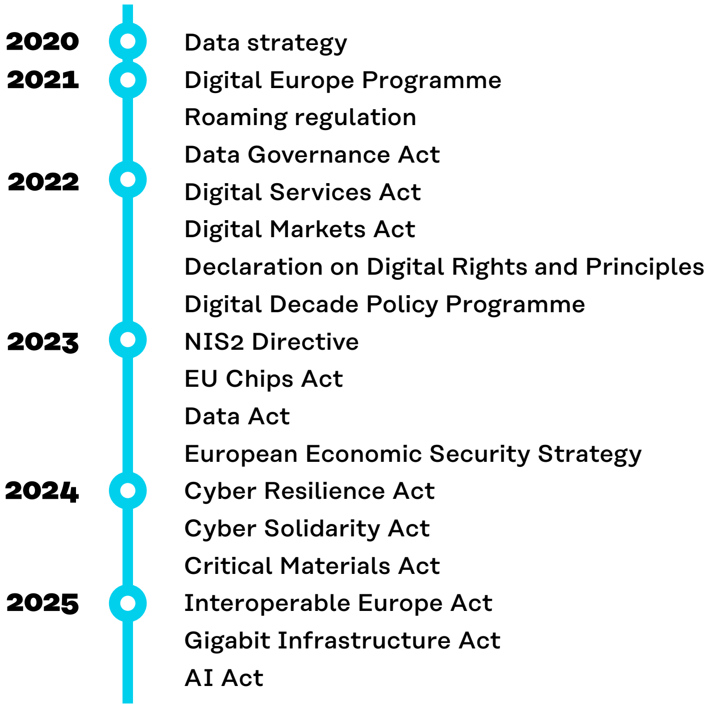
The EBA would become a flagship initiative of Europe's mindset adjustment: it represented a turning point from the traditional market-first approach of EU integration, towards strategic investment and EU-supported industrial cooperation, something long considered taboo under strict EU competition rules.

The Von der Leyen I Commission: the display of sovereignty

When Ursula von der Leyen became President of the European Commission in 2019, she placed geopolitics at the centre of her political agenda. The period 2019–2024 saw the digital agenda emerge as a distinct body of its own. The number of initiatives introduced during this period far exceeded those of her predecessor.

Von der Leyen's first term also represented a mentality shift inside the European Commission. The digital agenda should no longer mitigate single market risks but rather had to become a tool to shape markets in a way that reflects European values and protects European interests.

Figure 4. Overview of initiatives developed by the Von der Leyen I Commission



2020
Data strategy
2021
Digital Europe Programme
Roaming regulation
Data Governance Act
2022
Digital Services Act
Digital Markets Act
Declaration on Digital Rights and Principles
Digital Decade Policy Programme
2023
NIS2 Directive
EU Chips Act
Data Act
European Economic Security Strategy
2024
Cyber Resilience Act
Cyber Solidarity Act
Critical Materials Act
2025
Interoperable Europe Act
Gigabit Infrastructure Act
AI Act

The COVID-19 pandemic was a reality check on the EU's digital agenda. The interconnectedness of borderless digital infrastructures and open markets was no longer helping advance prosperity but rather had created new vulnerabilities with cascading effects reaching into all economic sectors. Connectivity issues and supply problems increased the awareness that regulations and policy initiatives, without industrial policy efforts, would not be able to deliver an EU capable of successfully managing risks.

Supply chain disruptions forced companies to reassess their value chains and replace suppliers, with others who were often located in distant geographies. These suppliers, few and scarce, were sometimes from countries that could weaponise their leverage on critical supply chains to pursue political interests. The production model that had previously enabled companies to scale and expand was now being called into question.

Dependency risks led to new initiatives to promote the reshoring and "friendshoring" of manufacturing and assembly, thus giving the EU respite from the disruption and redirecting interdependence from risky sources to closer and more stable partners. This explains the emergence of the digital partnerships with countries such as Japan (2022), Singapore (2023), Canada (2023), and South Korea (2024), and the establishment of the EU-U.S. and the EU-India Trade and Technology Councils (2021; 2023).

On the domestic front, the need to reconcile strategic autonomy ambitions with rising levels of self-reliance led to the release of flagship policies such as the EU Chips Act (2023), the Critical Materials Act (2024), and the Economic Security Strategy (2023). At the NATO level, such philosophy paved the way for the new Strategic Concept (2022), and new dedicated strategies in the realm of critical technologies such as AI (2021) or quantum.

Technological convergence in policy after COVID-19: The EU Chips Act

In February 2022, the European Commission proposed a European chips act package to decrease the reliance of the EU on foreign actors at different stages of the semiconductor value chain. It was a direct reaction to semiconductor shortages during the COVID-19 pandemic and an active effort to increase resilience by promoting initiatives in those supply chain areas where the EU was the most vulnerable. However, beyond semiconductors, the EU Chips Act proposed measures to improve European capacities in quantum chips, a technology still under development and where no single player has yet claimed a leadership position.

The EU Chips Act, approved in July 2023, is based on three pillars: 1) initiatives to reduce lead time and improve innovation from lab to fab; 2) measures to attract investment and improve domestic production capacities and 3) a coordination and response mechanism to respond to supply disruptions. For quantum chips, it paves the way for the creation of pilot lines and a design library.

The EU Chips Act implicitly recognises that quantum chips and semiconductors have a lot in common, including overlapping supply chains, and that both are parallel technologies playing a role in technology stacks. The Chips Act, therefore, by promoting horizontal measures for both semiconductor technology and quantum technologies indirectly influences technological convergence.

In addition to COVID-19, the Russian war of aggression against Ukraine in 2022 became another defining moment. It exposed the raw consequences of interdependence and overreliance, putting to the test some of the partnerships and measures the EU was developing in parallel. Bilateral fora, in particular the EU-U.S. Trade and Technology Council, were established to develop common approaches to technology governance problems. They proved essential for coordinating sanctions but also highlighted the vulnerabilities of governance initiatives that rely on political alignment rather than technical cooperation.

Faced with an increasingly antagonistic U.S., which hosts much of the technology innovation on which the EU depends, and with China as the only alternative, the EU adopted strategic autonomy as its approach to innovation: boosting domestic R&D and production – including in areas that strengthen European defence – while seeking new partnerships to reduce overreliance.

Strategic autonomy in action: the EU-U.S. Trade and Technology Council (TTC)

At the inaugural statement signed in Pittsburgh in September 2021, the EU and the U.S. pledged to work together on issues that were pre-regulation but were essential for both economies (European Commission, 2021a). At the same time, the EU-U.S. TTC was established to create a united front against the rise of authoritarian tech powerhouses such as China by promoting transatlantic trade and creating aligned technology policy frameworks.

During the first meeting, both addressed the need to work together on critical technologies setting the scene for further work on semiconductors and artificial intelligence (European Commission, 2021a). This was due to the shocks of the COVID-19 pandemic. However, the siloed and targeted approach to these two technologies failed to address risks of emerging applications, such as generative AI in cybersecurity, and data privacy, which only entered the discussion in 2023 at the Luleå TTC (White House, 2023), and quantum technologies, which also appeared much later. The TTC example highlights how initiatives that aim to create anticipatory governance frameworks need to address critical technologies from a point of convergence in order to foresee and prepare for the emergence of disruptive applications, both in terms of risk management and innovation implementation.

Critical technologies are the result of parallel processes that enable the development of essential building blocks often shared with other technologies, such as computer chips that are necessary in HPC, artificial intelligence, and many others. Managing interdependencies and growing a competitive technology industry requires managing relations to reduce dependencies, while also understanding how political and social factors influence their development.

From labs to the market: technological convergence through maturity

Maturity can serve as a strong indicator of the development level of critical technologies by defining the steps from proof of concept to market, while also providing a way of identifying potential opportunities for future convergence. In this context, technological maturity refers to the stage reached by a technology when it is sufficiently advanced for mass commercialisation and distribution to the general public.

To assess a particular technology's level of maturity, it is vital to determine its readiness for general implementation without major potential risks which may undermine its overall reliability. While maturity levels can be stable over time, the intersection of distinct technologies can generate innovations and give rise to new use cases. Thus, defining technological convergence through the lens of maturity provides a structured framework for analysing how different applications emerge at the intersection of technologies.

Although it is difficult to elaborate a general definition comprising all cases, this paper acknowledges the need for a broad definition, which could enable a deeper understanding of how convergence may occur among the main critical technologies and reveal opportunities that emerge at their intersection (European Commission, 2023a). Accordingly, it conceptualises technological maturity as the culmination of three distinct phases:

Phase 1: Basic research and early technological development

The development phase refers to the stage of experimentation and applied research that leads to the identification of suitable applications. Scientists and researchers focus on solving key technical problems and demonstrating their usability. Often, these tests happen outside the laboratory, but they do not necessarily provide a significant advantage over existing processes and applications in the market. Initial costs far outweigh the expected benefits during this period, and performance remains complex and precarious. Quantum technologies are still in this phase, as well as other advanced cyber-security solutions such as post-quantum cryptography and generative AI-powered cyber defence.

For instance, by anticipating the need to secure hardware from quantum attacks on encryption, SEALSQ, a Swiss company offers semiconductors that integrate post-quantum cryptographic algorithms. The goal is to provide a secure core for powering future digital infrastructure, although the firm is currently positioning their quantum-secure chips to power decentralised AI systems (SEALSQ, 2025). This example demonstrates how ideas born at the intersection of critical technologies, even in the development phase, can create high-value applications with positive spillover effects throughout the technology stack.

Phase 2: Growth and exploration of first market applications

This stage is characterised by the rapid emergence of innovations that enhance the technology's operability. Consequently, it becomes more cost-effective, and its improved performance enables distribution and commercial applications – albeit not yet on a large scale. However, it is during this phase that 'winter' periods may occur.

A state of stagnation in innovation breakthroughs, and in adequate investment, can reduce the speed of development. Advanced connectivity solutions or artificial intelligence are arguably in a growth phase under this definition, with breakthroughs such as generative AI making headlines.

Companies such as KONUX in Germany are putting together hybrid solutions combining different technologies at the growth stage. KONUX combines artificial intelligence with IoT solutions to deliver real-time insights about the state of transportation networks (KONUX, 2025). This enables administrations to anticipate maintenance operations and plan services more effectively. In addition, knowledge about network health and usage supports the development of the more sustainable use of transportation links, contributing to the advancement of the green agenda.

Phase 3: Commercial maturity

At the stage of maturity, the technology becomes fully reliable and operational risks are minimal. Distribution is cost-effective and it has proven advantages over traditional methods, allowing for widespread utilisation. Often, new technologies reaching maturity can replace older ones, rendering them obsolete thanks to their effectiveness and practicality, and may become ubiquitous thanks to their competitive advantage (e.g. email replacing letters).

Once a technology reaches maturity, breakthroughs are rare, and they seldom change the fundamentals on which the technology is built. Instead, advancements are sought in terms of operational upgrades. In general terms, semiconductor technology, cybersecurity solutions, and space technologies belong to this category.

WithSecure is a Finnish company delivering advanced cybersecurity solutions through the cloud––two established technologies at the Critical Core––often in combination with artificial intelligence (WithSecure, 2025). This example shows that even in two innovative, but mature, digital industries (cybersecurity and cloud), convergence appears to create new links and applications. While there may be fewer breakthroughs than if the technologies were still in the growth phase, valuable hybrid applications and solutions still emerge.

Technological convergence, as viewed from the maturity scale of new technology sectors, is an opportunity to create investment opportunities for technologies that are still at the basic research phase. Moreover, a convergence mindset can help accelerate the development of those technologies that are still growing while increasing new market opportunities in technology sectors that are seen as more mature. Technology convergence is not merely a matter of chance; it can be actively cultivated to ensure that industries and countries maximise the use of available resources, including talent, data, and infrastructure.

From policy to solutions: technological convergence through innovation structures and culture

New technological applications cannot reach maturity without the structures and culture to support them. Technological development is inherently intertwined with the social and political contexts in which innovation emerges. Factors such as geopolitics, domestic dynamics, and the prevailing culture of innovation all play a crucial role in determining research and experimentation priorities. Changes in any of these dimensions can have lasting implications for a country or region's ability to remain at the forefront of technological revolutions. Therefore, technologies should be understood as context-dependent, rather than isolated from the environment in which they are developed.

Geopolitical risk shapes political and economic relations significantly, with direct implications for innovation and the development of new technologies. While geopolitical uncertainty tends to dampen private-sector innovation, with firms being more risk-averse and scaling back investments in transformative technologies (Astvanash, Deng, & Habib, 2022), the effect on state-driven innovation is more complex.

In contrast to the chilling effect of international uncertainty on privately led innovation, state-backed innovation often accelerates in a scenario of crisis and geopolitical pressure, particularly at a time when technology increasingly plays a role in the definition of power (Noël, 2019). Perhaps the most paradigmatic example is the internet, which emerged from the development of ARPANET (DARPA, 2025), a 1960s project conceived by the U.S. Department of Defence. Born out of the imperative of safeguarding critical communications between distant U.S. territories during a potential nuclear attack, DARPA led to the development of packet-switching technology, designed to prevent information loss even if a network node were to fail. This efficient and scalable technology, developed during a period of intense geopolitical strain, is fundamental to understanding modern networks and the digital technologies emerging from them.

Table 1. Impact of geopolitics and political stability on the development of new technologies based on policy review

	Peaceful geopolitics	Geopolitical tensions
Political stability	• Boost in strategic planning • Surge in private investment • Surge in public investment across the maturity scale (including low TRL and basic fundamental research)	• Strategic planning driven by the mitigation of risks • Contraction of private investment • Public targeted investment in high impact and near-market applications
Political instability	• Lack of organised long-term investment planning • Decline in private and public investment • Focus on near-application technologies that benefit political cycles	• Priority shift from long-term threats to short-term threats. • Low planning; innovation may not be a top political priority • Decline in private investment • Lower public investment

While geopolitics certainly plays a role, domestic political dynamics, including the capacity to make long-term commitments and the nature of political systems, are equally critical. Conceptions about legality and ethics in innovation, as well as interpretations of the "state interest" shaped by internal power structures, strongly influence not only which innovations receive support, but also how technology applications are tested, experimented with, and ultimately implemented.

In global comparison, China's approach to innovation emphasises long-term, government-directed policies and instruments to enhance technological innovation in desired areas. In contrast, the United States upholds a market-driven approach with policy initiatives potentially emerging later based on market insights. The European Union, an actor with unique characteristics, can combine success stories from both models: using its strong foresight capacity and market relations to ensure that policy action guides, not creates or responds to, innovation. State-directed economies sometimes have an advantage in terms of long-term planning, as they are not constrained by political debate or the need to build consensus among competing political parties. The emphasis placed on innovation by economists and political leaders as a key driver of economic growth helps explain the current geopolitical competition for technological breakthroughs, as the future increasingly revolves around the contest for ideas.

Until recent years, Europe and the United States had been at the forefront of the technological wave with world-leading research institutions and universities, a surge in investment, and a favourable regulatory environment. However, the rapid rise of Chinese investment capacity has opened the debate on whether democracies can keep up. To thrive in a world of authoritarian innovation where traditional EU-U.S. relations are under strain, the EU must rethink its financial frameworks for innovation, accelerating decision-making processes. This should be accompanied by increased support for exploring technological convergence, which may not yield immediate results, but prove critical for maintaining Europe's competitiveness and international influence.

3. Technological convergence in practice

Innovators naturally embrace technological convergence as an opportunity to increase competitiveness. Technological convergence is not a concept of the future, but a current trend that is already shaping the future of critical technology sectors.

Innovation is inevitably at the centre of various debates currently shaping the EU's digital agenda, ranging from competitiveness, exemplified by the Draghi report (2024), to the creation of a "fifth freedom" in the single market as highlighted in the Enrico Letta Report (2024), and improving European defence, a topic explored by the former Finnish president Sauli Niinistö (2024). Access to, control over, and the development of critical digital technologies are fundamental to achieving a resilient, safe, and prosperous Europe.

The interdependencies between digital technologies at the Critical Core (see: Figure 1), such as semiconductors, cloud infrastructure, and artificial intelligence, have had a significant impact on the EU's strategic autonomy. These technologies, far from being independent clusters, form a tightly woven ecosystem in which developments in each of them impact innovation and growth capacity in the others.

This impact can be represented in two ways. Numerous digital technologies have overlapping value chains, leading to advancements in a certain technology cluster (e.g. cybersecurity), which has cascading effects on other technologies from a supply chain perspective (e.g. data). Thus, incentives tailored for one specific industry often spill over into others, creating opportunities for the growth of new sectors (World Economic Forum, 2025, pg. 9). Technological convergence affects value chain resilience, enabling actions and measures to extend their intended impact throughout the Critical Core.

Furthermore, technological convergence favours the creation of applications at the intersection of different technologies that, as explored in the preceding chapter, are well-positioned for breakthrough. This so-called "compounding effect" (World Economic Forum, 2025, pg. 11) of technology, benefits from complementary innovation happening at different stages of development. The development of these positive effects can be incentivised through regulation.

Numerous debates are currently underway on ways to improve Europe's strategic autonomy when it comes to technology. Many of the debates are centred around the idea of building a European technology stack to reduce dependency on foreign technologies and applications (e.g. Bria et al., 2025). While having a stack-centric approach can help understand Europe's vulnerabilities and increase the coordination of investment efforts, these capacity-building initiatives will inevitably need to consider technological convergence.

Case 1: Physical AI

Digitalisation is the foundation of cyber-physical ecosystems that enable the connection and mapping of the physical world into the digital realm (European Commission, 2021b). This convergence underpins the efforts to integrate AI solutions into biologically inspired machines or 3D-printed robots by blending sensors, actuators, and machine learning. Physical AI can be defined as the resulting interface that combines advanced manufacturing solutions with AI solutions, noting that advanced manufacturing and AI are key for Europe's competitiveness and economic security.

Physical AI systems expose new challenges in scalability and integration. Hardware costs and complexity can limit production, particularly for scaling microrobots and bio-hybrid devices, which often lack established mass-manufacturing routes. 3D printing can be part of the solution by lowering costs and enabling easy access to technology developments. Moreover, physical control and AI must cope with real-world uncertainty, which is a complex generalisation problem affecting AI systems deployed in real-life environments. Outside the lab, scenarios are hard to predict, and so, in combination with the robotic body, adaptation is sometimes an issue in the deployment of physical AI.

However, physical AI offers a wide range of opportunities to be deployed where humans cannot operate naturally. For instance, in biodiversity conservation, physical AI can play an essential role in helping ecosystems adapt to changes in the biosphere. The RoboRoyale project is an example of this, founded under Horizon 2020 (see Table 2), and is working to develop micro robotic bees guided by machine learning to support honeybee queens.

Table 2. Convergence in practice: Projects funded by Horizon 2020 and Horizon Europe at the intersection of AI and robotics.

Project name	Launch date	Description
RoboRoyale	November 2021	Develops micro robotic bees guided by machine learning to support honeybee queens. Blends 3D-printed microrobots, biological sensing and AI control to sustain ecosystems.
I-Wood	May 2021	Builds virtual and physical robotic networks that mimic the plant fungus 'wood wide web'. Biologically inspired robot roots sense and grow, combining plant science with AI and robotics.
CONVERGING	September 2022	Creates smart manufacturing systems with multiple agents (robots, AGVs, humans). Uses AI and big data to self-diagnose and reconfigure production hardware, enabling human-robot collaboration.
AI-PRISM	September 2022	Human-centred AI ecosystem for factories. Builds a programming-by-demonstration platform so that AI-driven robots can flexibility perform diverse tasks without expert coding.
REGO	October 2022	Introduces AI-powered microscale robot swarms. Tiny modular robots, wirelessly controlled via AI and intuitive interfaces, cooperate on tasks such as medical micro-interventions.
SOPRANO	October 2023	Advances human-robot teaming in industry. Develops multi-agent robotic systems that adapt to dynamic environments, scaling from single robots to networks of intelligent machines.

Technical problems linked to scalability, as mentioned above, and a fragmented policy landscape, are limiting the uptake of physical AI solutions and the investigation of new use cases. Different EU Member States have varying robotics strategies, and investment levels also differ, which can lead to the duplication of efforts and the creation of R&D gaps. On top of this, Europe's smaller market for venture capital means scaling proof-of-concept systems into marketable products is more challenging in the EU than in the U.S. and China.

However, on the positive side, EU funding programmes support the convergence of advanced manufacturing and AI. Nonetheless, the topic remains underexplored in policy discussions. In 2020, there was a draft proposal (European Commission, 2020) for a European Partnership on AI, Data and Robotics under Horizon Europe. However, several years after its approval in 2021, no progress reports have been published. The last overview of the situation at the end of 2023 indicates that no participants or countries have joined the Partnership, which is intended to run until the end of 2030 (ERA-LEARN, 2025).

An overview of initiatives supporting the convergence of several critical technologies (see: Annex 1) demonstrates that while EU policy increasingly addresses convergence, advanced manufacturing is largely omitted from the scope. Despite sectoral advancements in the fields of AI or data, physical AI is far from becoming a reality and has yet to attract the necessary attention from the European Commission. In addressing varied challenges from loss of biodiversity to security and defence, physical AI is a next step for AI models, giving them body and allowing AI to give shape the physical world.

Case 2: Artificial intelligence and cybersecurity

The complex relationship between artificial intelligence and cybersecurity, particularly their mutual convergence, is only explored briefly in regulation. Artificial intelligence can be especially useful in threat detection and automated threat response. Indeed, the NIS2 Directive, the EU's most significant cybersecurity legislation, makes a reference to AI when encouraging member states to leverage "innovative technology, including artificial intelligence, the use of which could improve the detection and prevention of incidents" (Recital 51, NIS2 Directive, see more details in Annex 1), as well as in relation to active cybersecurity. It does not, however, make it mandatory in any form.

An interesting correlation exists between how AI for cybersecurity is addressed in policy documents and how it is addressed by funding instruments. The table below summarises the projects funding the creation of AI solutions to improve cybersecurity under the Horizon programme. Although these descriptions offer an understanding of the opportunities of creating hybrid applications at the intersection of AI and cybersecurity, much remains to be done to promote not only the development of these hybrid solutions, but also their implementation into the cybersecurity resilience cycle. This remains a key task for policymakers.

Companies such as Darktrace (UK) and Palo Alto Networks already offer AI-powered cybersecurity solutions. However, despite the EU's leadership in cybersecurity governance, available funding to enhance cybersecurity protection, and the vibrant cybersecurity ecosystem, no EU company currently leads this space.

This example highlights the necessity of frameworks for convergence, as well as the need to raise awareness about innovation in the policymaking community. As this brief analysis shows, there appears to be a disconnection between how the EU thinks about cybersecurity and how industry thinks about cybersecurity, with the latter being more innovation-driven and willing to take new risks by exploring convergence with artificial intelligence.

Table 3. Convergence in practice: projects funded by Horizon 2020 and Horizon Europe at the intersection of AI and cybersecurity

Project name	Launch Date	Description
IRIS	03 May 2021	Developing an AI threat reporting and incident response system to support CERTs/CSIRTs operations.
STARLIGHT	21 May 2021	Improving understanding of AI across law enforcement agencies to reinforce investigative and cybersecurity operations.
AI4CYBER	04 September 2022	Providing an ecosystem framework of next-generation cybersecurity services leveraging AI and Big Data.
PHOENI2X	12 September 2022	Developing AI-assisted situational awareness, prediction capabilities, and resilience orchestration for business continuity and incident response.
Sec4AI4Sec	14 July 2023	Developing security-by-design testing and assurance techniques for AI-augmented systems to address security challenges.

Case 3: Semiconductors

Another example that highlights how exploring technological convergence has driven the EU digital strategic autonomy agenda forward can be seen in its global partnerships to address semiconductor shortages. However, in this case, the strategy needs to be complemented with external action, given that the EU lacks advanced capabilities in this domain.

Strategic autonomy acknowledges that full technological self-sufficiency is neither feasible nor desirable. Instead, it focuses on securing control over strategic supply chains, including essential components and services. In the EU, investments in semiconductors follow the EU Chips Act (2023), building on the Important Project of Common European Interest (IPCEIs) state aid framework. IPCEIs bring together private companies and at least two EU Member States to deliver large-scale, co-financed projects that foster innovation, infrastructure and clusters in strategic industrial sectors, generating positive spillover effects such as growth, competitiveness and employment.

The European Semiconductor Manufacturing Company (ESMC), a joint venture in Dresden between TSMC (Taiwan), Bosch (Germany), NXP (Netherlands), and Infineon (Germany), has a positive impact on the development of the Critical Core, particularly on artificial intelligence, high-performance computing, and 6G networks (ESMC, 2025). TSMC's technology can compensate for lagging European cutting-edge computer chip technology to develop advanced AI applications, while the partnership with German and Dutch companies improves resilience in the event of external shocks. However, this partnership remains highly dependent on public subsidies. While it addresses supply security issues and boosts the EU's production capacity, it neither ensures independence from geopolitical tensions in the Taiwan Strait nor guarantees technology transfers.

For this reason, aligned with the Digital Compass (European Commission, 2021b), which prioritises digital infrastructure, the EU has invested in digital partnerships in East Asia, where semiconductor manufacturing is largely concentrated. Since 2023, it has engaged Japan, an essential player in the upstream segment of the semiconductor supply chain, through a Digital Partnership Council. In 2024, the EU expanded its digital engagement with South Korea, a global leader in downstream chip manufacturing. As part of this partnership, the EU and the Republic of Korea launched four jointly funded projects to promote innovation and research in semiconductors (European Commission, 2024), where scientific cooperation is facilitated through the EU-Korea Semiconductor Researcher Forum.

Moreover, the June 2025 EU International Digital Strategy acknowledges the need to invest in deepening, broadening, connecting, and strengthening partnerships around the globe to support its goals (European Commission, 2025a). The operationalisation of this vision, along with efforts to revive the EU's chip industry in line with its goals for emerging technologies—such as in quantum computing and artificial intelligence—will be crucial to ensuring that the benefits arising at the intersection of mature sectors such as semiconductors and emerging industries have a positive impact on the EU's digital economy.

While technological convergence may not drive EU policymakers' thinking when engaging with international partners, the EU has effectively realised that to be a credible actor in critical technologies, it must secure the supply of shared essential building blocks.

4. Recommendations and conclusions

Harnessing the power of technological convergence is not a matter of reshaping how the EU functions but rather rethinking how the EU drafts and implements policies and instruments, making foresight a critical pillar of the digital agenda.

As new solutions and applications draw from digital technologies, systemic approaches to technology must prevail. However, the sector-specific—or "innovation-specific"—nature of current frameworks of governance makes convergence something that happens by chance, instead of being deliberately acknowledged. Still, technological convergence, as seen in the examples in the chapters above, is inevitable.

The approach to technology policy has shifted in the last decade as debates around Europe's position in the race to control infrastructure and data have increasingly unfolded. Strategic autonomy, viewed as a cumulative process influenced by external events—such as the birth of the platform economy—has played a significant role in accelerating EU digital policy and transforming the use of policy instruments from tools to correcting market errors into instruments for shaping emerging markets.

Breakthroughs that are true industry-shapers have happened and will continue happening at the intersection of different technological clusters. Emerging technologies often share critical building blocks, infrastructure, and talent. Therefore, promoting convergence, instead of the takeover of a single technological cluster, will have positive spillover effects into the network of interacting technologies. So far, as the analysis demonstrates, policy has been directed towards the opposite approach, with targeted initiatives aimed at making Europe a leader in specific technologies, rather than focusing on the hybrid applications that enable the Critical Core.

There is no direct correlation between how the market, innovators, and policymakers view convergence. Opportunities abound, but the willingness to exploit them is limited, requiring a shift in mentality. Understanding and identifying this gap is crucial not only for recognising the potential of adopting a technological convergence approach, but also for detecting regulatory gaps, duplications and overlaps that can hinder—rather than promote—innovation in critical digital technologies.

Table 4 presents a wide array of applications that are the result of convergence happening at the Critical Core. It visualises them using a heatmap that indicates how close these hybrid applications are to commercialisation. Blue indicates hybrid applications such as the use of advanced semiconductors for satellite imaging, and the use of AI in powering adaptive threat detection and response. Yellow represents hybrid applications such as the use of AI to generate traffic in 5G/6G cells, or the provision of quantum-safe encryption and uplink/downlink capabilities for mega-constellations of satellites. These examples of applications will power European innovation for decades, themselves enabling new applications further down the line.

Table 4: Synergies between critical digital technologies (Technology Industries of Finland, 2025) and heatmap representing close-to-market synergies between different critical digital technologies: blue applications are estimated to be close to market (< 3 years), while yellow positions it in the near future (3 to 7 years).

Enables/ depends on	AI	HPC	Semiconductors	Quantum	Space	Connectivity	Cybersecurity	Data
AI	-	Requires large-scale training on supercomputers	Drives demand for specialised chips	Supplies error-mitigation and optimisation algorithms for quantum devices	Provides on-board analytics and autonomy for satellites	Generates traffic for 'edge AI' in 5G/6G cells	Powers adaptive threat detection and response tools	Requires plentiful, high-quality datasets
HPC	Accelerates AI model training and interference	--	Depends on cutting-edge semiconductor nodes	Performs quantum-system simulation and error-correction workloads	Processes vast Earth-observation datasets from space missions	Feeds ultra-fast 'edge' computation close to 5G/6G base-stations	Must be shielded against intrusions and data leaks	Processes petabyte-scale inputs
Semiconductors	Supplies AI-specific chip designs	Provides high-bandwidth memory for supercomputers	---	Enables control electronics that operate at cryogenic temperatures for quantum chips	Provides radiation-hardened components for spacecraft	Produces radio-frequency front-end components for 5G/6G	Integrates secure-by-design hardware 'roots of trust'	Integrates on-chip data protection features
Quantum	Works with AI to solve complex optimisation tasks	Uses HPC clusters for quantum-circuit simulation	Relies on ultra-pure semiconductor fabrication lines	--	Hosts space-based quantum key distribution links	Requires synchronised, low latency 5G/6G channels for control	Provides quantum-safe encryption	Requires high integrity verified datasets
Space	AI interprets high-resolution satellite imagery	HPC fuses data from numerous on-orbit sensors	Uses advanced semiconductors for imaging sensors and payloads	Will carry quantum repeaters and atomic clocks	--	Offers satellite backhaul for 5G/6G in remote areas	Demands secure 'telemetry, tracking & command' links	Generates geospatial, big data streams
Connectivity	Brings real-time data to AI at the network edge	Interconnects geographically distributed HPC centres	Requires dense input/output and phased-array radio chips	Can transport quantum keys over optical-fibre or free-space links	Provides up-and-down links for mega-constellations of satellites	---	Requires end-to-end secure 'network-slicing' and 'multi-access edge computing'	Streams massive, distributed datasets
Cybersecurity	Protects the AI supply chain and trained models	Secures supercomputers, job schedulers and data	Ensures trusted semiconductor intellectual property	Develops encryption resistant to quantum attacks	Protects navigation and satellite payload links	Hardens network slices, base stations and edge nodes	---	Maintains data integrity, authenticity, and privacy
Data	Determines AI accuracy fairness and bias	Influences the reliability of scientific simulations	Guides semiconductor process control and yield improvement	Trains hybrid quantum-classical systems	Supports Earth-observation-based climate insights	Optimises traffic flow in 5G/6G cores	Needs confidentiality provenance and verifiable lineage	---

At a time when foundational technologies such as data and semiconductors are advancing rapidly, technological convergence is increasingly coming to the forefront. Given the new budget cycle and the accelerating challenges—from global geopolitics and the responsible development of critical technologies to securing supply chains—the EU must take bold measures to put technological convergence at the forefront of policy discussions.

Policy recommendation 1: Reduce fragmentation in funding schemes affecting critical digital technologies and establish clear research-to-market pathways

The siloed approach to technology often creates competing funding packages that foster the emergence of well-defined applications but limit the development of hybrid applications, as researchers and companies must choose where to focus.

For this reason, and in light of the Commission's efforts to fund critical technologies, discussions under the 2028–2034 Multiannual Financial Framework (MFF)—particularly the EU Competitiveness Fund—must take technological convergence into account. This will enable instruments created through this initiative to fund hybrid applications, thus allowing the EU to simultaneously accelerate on multiple fronts.

However, maintaining a wider scope in the funding calls will be essential to ensuring that EU instruments can accommodate hybrid applications. The current detailed focus and narrow definition of funding calls reduce the ability of hybrid scientific communities (e.g. quantum software engineers working on advanced AI) to access EU funding, which in turn hinders the EU's ability to attract and retain valuable talent. Furthermore, to ensure that innovation funded by the EU is used, there should be clear provisions to guarantee that these applications reach the market after the project period. For this to happen, the EU should work on establishing partnerships with the private sector and use public procurement to test, deploy, and use EU-born innovation.

Policy recommendation 2: Prioritise highly convergent technologies while using public funding

Technology development is the result of systemic changes and the networked interactions of different clusters, as exemplified by the Critical Core, and addressed in this study. However, not all technologies generate the same spillover effects across sectors. For this reason, prioritising high-impact, highly convergent applications that benefit European wellbeing and security will be key to generating cascading effects across the clusters in the Critical Core. Currently, these include quantum technologies at the infrastructure/hardware level, AI—in the software/logical layer, and data, which powers information exchange between layers. Any change to this list of technology should be closely linked with clear and structured foresight activities.

Policy recommendation 3: Introduce technological convergence as a mandatory aspect in impact assessments

While the mix of geopolitical uncertainty and political stability at the EU level is driving new initiatives for domestic innovation, these initiatives either focus on identifying critical technologies based on their disruptive potential and their level of critical dependency on foreign actors, or on boosting the sectoral development of these technologies.

However, these analyses often overlook cross-sectoral opportunities, limiting the appearance of hybrid/convergent applications. Addressing convergence in future impact assessments will enable the EU to build a cohesive policy framework with simultaneous positive spillover effects on multiple technologies, while identifying areas where further policy action is needed.

Policy recommendation 4: Coordinate efforts to publish annual foresight reports on technological convergence in the EU

The EU has made solid efforts in recent years to map and identify critical technologies and has a strong network of research bodies such as the Joint Research Centre and the European Parliament Research Service (EPRS). However, despite the development of solid methodology and noteworthy studies, often done so in collaboration with external actors, technological convergence remains an underexplored topic. Precisely because of the strong in-house capacities and network of researchers that the EU can mobilise, it should leverage these strengths to publish annual reports on the state of technological convergence. This foresight exercise will prove fundamental in ensuring that funding is aligned with economic security priorities and fine-tune the ability of the EU to navigate future risks and shocks.

Moreover, it will be crucial to ensure that policymakers participate in the foresight process to guarantee that the work is useful and a driver of future policy action. Ensuring that the relevant Directorate Generals are involved will inevitably also mean the participation of the appropriate personnel: heads of unit, deputy heads of unit, and/or team leaders.

Conclusions

Increasing European competitiveness and strategic autonomy requires a comprehensive view of critical digital technologies and an understanding of their value chains. Technology sectors should not be treated individually, but rather analysed through their intersections with other fields, as well as their social and political settings.

As a governance concept, technological convergence obliges actors to consider the contextual effects of regulatory, policy, and funding approaches to technology. For the European Union, this approach requires an emphasis on strategic funding based on technological foresight. Siloed approaches, based on how the European Commission currently organises its work and funds innovation, are insufficient to address the systemic opportunities and also challenges of industries that are, by nature, networked across multiple sectors and technologies.

In a world of multiplying challenges requiring rapid responses, embracing technological convergence can help the EU make better use of available resources, enhance its competitiveness across multiple technology sectors, and identify new opportunities for leadership in areas emerging at the intersection of technologies.

References

Astvanash, V., Deng, W., and Habib, A. 2022. Research: When Geopolitical Risk Rises, Innovation Stalls. Harvard Business Review (retrieved 19 July 2025).

Bria, F., Timmers, P., Gernone, F., Renda, A., Fischer, C., Grabova, O. 2025. EuroStack—A European alternative for digital sovereignty. Centre for European Policy Studies (CEPS).

DARPA. 2025. ARPANET. (PDF).

Draghi, M. 2024. The Future of European Competitiveness. (PDF).

ERA-LEARN. 2025. Partnerships. AI-Data-Robotics. (retrieved 1 August 2025).

European Commission. 2015. A Digital Single Market for Europe: Commission sets out 16 initiatives to make it happen. (retrieved 28 July 2025).

European Commission. 2017. White Paper on the Future of Europe. COM(2017)2025 Final. (retrieved 28 July 2025).

European Commission. 2020. Draft proposal for a European Partnership under Horizon Europe: AI, Data and Robotics. (PDF).

European Commission. 2021. Remarks by Executive Vice President Dombrovskis on Fostering the Openness, Strength and Resilience of Europe's Economic and Financial System. Press Corner. (retrieved 28 July 2025).

European Commission. 2021a. EU-US Trade and Technology Council Inaugural Joint Statement. Press Corner. (retrieved 1 August 2025).

European Commission. 2021b. European Partnership under Horizon Europe. Key Digital Technologies. (PDF).

European Commission. 2021b. 2030 Digital Compass, the European way for the digital decade. COM(2021) 118 final. (retrieved 29 August 2025).

European Commission. 2022. Factsheet: Japan–EU Digital Partnership. Press Corner. (retrieved 25 July 2025).

European Commission. 2023. Factsheet: EU–Singapore Digital Partnership. Press Corner. (retrieved 25 July 2025).

European Commission. 2023a. Commission recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States,. C(2023) 6689 final. (PDF).

European Commission. 2024. EU–Republic of Korea Digital Partnership— Joint EU/Republic of Korea Chips Projects Announced. Press Corner. (retrieved 25 July 2025).

European Commission. 2025. EURAXESS, TRL. (retrieved 1 August 2025).

European Commission. 2025a. Joint Communication on an International Digital Strategy for the EU, Library. (retrieved 01 August 2025).

European Parliament. 2024. EU-India Trade and Technology Council. At a Glance. (retrieved 29 August 2025).

European Semiconductor Manufacturing Company. 2025. Who we are. (retrieved 29 August 2025).

Government of Canada. 2023. Canada–European Union Digital Partnership. (retrieved 25 July 2025).

Government of China. 2015. Report on the Work of the Government. (retrieved 25 July 2025).

KONUX. 2025. About us. (retrieved 29 August 2025).

McKinsey & Company. 2020. McKinsey Electric Vehicle Index: Europe Cushions a Global Plunge in EV Sales. (retrieved 21 July 2025).

Niinistö, S. 2024. Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness. (PDF).

Noël, J.C. 2019. What is Digital Power? Institut Francçais des Relations Internationales (IFRI). (retrieved 21 July 2025).

Letta, E. 2024. Much More than a Market: Speed, Security, Solidarity. Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens. (PDF).

SEALSQ. 2025. About us. (retrieved 29 August 2025).

Timmers, P. 2025. Strategic autonomy and the EU. A short history. European Cybersecurity Journal, volume 10, pp. 53-67.

Timmers, P. 2024. Sovereignty in the Digital Age. In: Werthner, H., et al. Introduction to Digital Humanism. Springer, Cham, pp. 571-592.

White House. 2023. US-EU Joint Statement of the Trade and Technology Council. Briefing Room. (retrieved 21 July 2025).

WithSecure. 2025. Solutions. (retrieved 29 August 2025).

World Economic Forum. 2025. Technology Convergence Report. (retrieved 01 August 2025).

Annex 1: Review of critical digital technologies addressed in the EU and Finland

This annex aims to provide the reader with an overview of the policies that affect several critical digital technologies and that have been considered as empirical input for this study. The cap for these policies is May 2025, so new policies appearing after that date might not have been considered. This annex shows that technological convergence is increasingly entering political discourse in both the EU and Finland. However, without a clear framework, states are poised to benefit from convergence only by chance, which limits the positive impact and spillover effects that embracing this approach can have for Europe's economic security.

European Union

Policy	References within
AI Act (2024) Main domain: artificial intelligence Subsidiaries: data, cyber	Data **Art. 10: Data and Data Governance** **Art. 17 (f)**: Providers of high-risk AI systems shall put quality management systems in place : procedures for data management, including data acquisition, data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other data operation that is performed before, and for the purpose of, placing high-risk AI systems on the market or putting them into service. **Article 71**: EU Database for High-Risk AI Systems Listed in Annex III. Cybersecurity **Art. 15: Accuracy, Robustness and Cybersecurity** **Art. 78**: Confidentiality.
Secure Connectivity Programme Regulation (2023). Main domain: space Subsidiaries: quantum, data	Quantum **Art. 3(c) and 4(c)**: Develop further and gradually integrate EuroQCI into the secure connectivity system. **Art. 28(d)** on the role of the ESA. Quantum + cybersecurity **Recital 15**: One of the main functions of the EuroQCI will be to allow for QKD. To date, QKD technology and products are not sufficiently mature to be used for the protection of EU classified information (EUCI). The main issues concerning QKD security, such as standardisation of QKD protocols, side channel analysis, and evaluation methodology, still need to be solved. The Programme should therefore support the EuroQCI and allow for the inclusion of approved cryptographic products in the infrastructure when available. **Art. 30.2**: The Commission shall consult the Council and the Member States regarding the specification and design of any aspect of the EuroQCI infrastructure, in particular the QKD that relates to the protection of EUCI. Cybersecurity Art. 3(e): One of the objectives is to increase the robustness of the Union's and the Member States' communication services and the cyber resilience of the Union, by developing redundancy, passive, proactive and reactive cyber protection and operational cybersecurity and protective measures against cyber threats and other measures against electromagnetic threats. **Art. 30**: Governance of security 30.1: The Commission shall, within its field of competence and with the support of the Agency, ensure a high degree of security. Data **Art. 8: Environmental and space sustainability** 8.1.(e): Submission and implementation of orbital positioning data for a comprehensive mitigation plan regarding space debris. 8.2: Obligation to provide data, in particular ephemeris data and planned manoeuvres. 8.3: The Commission shall ensure that a comprehensive database of the Programme's space assets, containing, in particular, data relating to environmental and space sustainability aspects, is maintained. **Art. 44: Personal data and privacy protection**

Policy	References within
Digital Markets Act (2022) Main domain: data Subsidiaries: cyber	Data (protection) **Art. 5: Obligations for gatekeepers** 5.2: The gatekeeper shall not (a) process, for the purpose of providing online advertising services, personal data of end users using services of third parties that make use of the core platform services of the gatekeeper; (b) combine personal data from the relevant core platform service with personal data from any further core platform services or from any other services provided by the gatekeeper or with personal data from third-party services; (c) cross-use personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services, and vice versa. **Art. 7.8**: The gatekeeper shall collect and exchange with the provider of number-independent interpersonal communications services––who request interoperability––only the personal data of end users that is strictly necessary to ensure effective interoperability. Any such collection and exchange of the personal data of end users shall fully comply with Regulation (EU) 2016/679 and Directive 2002/58/EC **(GDPR + e-privacy)**. Data protection + security **Art. 7.9**: The gatekeeper shall not be prevented from taking measures to ensure that third-party providers of number-independent interpersonal communications services requesting interoperability do not endanger the integrity, security and privacy of its services, provided that such measures are strictly necessary and proportionate and are duly justified by the gatekeeper. Cybersecurity / end-to-end encryption **Art. 7.3**: The level of security, including the end-to-end encryption, where applicable, that the gatekeeper provides to its own end users shall be preserved across the interoperable services. **+7.4** relating to the reference offer on technical details and general terms and conditions of interoperability the gatekeeper shall publish.
Digital Service Act (2022) Main domain: data Subsidiaries: cyber	Data **Art. 15 & 23**: 'Transparency reporting obligations for providers of intermediary services' and 'Measures and protection against misuse' imply that providers of online platforms have **record keeping obligations** (i.e. data traceability). 15.1: Providers shall make publicly available, at least once a year, clear, easily comprehensible reports on any content moderation that they engaged in during the relevant period. 23.3: Providers shall regularly provide data on misuse, including: absolute numbers of items of manifestly illegal content or manifestly unfounded notices or complaints, the gravity of the misuses, including the nature of illegal content, and of its consequences; when possible, the intention of the recipient of the service, the individual, the entity or the complainant. **Art. 40: Data access and scrutiny** VLOPs must provide data that is necessary for vetted researchers to conduct research on risks posed by their services. **40.12: + cybersecurity**: Providers of VLOPs and VLOSEs shall give access without undue delay to data, including, where technically possible, to real-time data, provided that the data is publicly accessible in their online interface by researchers, including those affiliated with not-for-profit bodies, organisations and associations, who comply with the conditions set out in paragraph 8, points (b), (c), (d) and (e), and who use the data solely for performing research that contributes to the detection, identification and understanding of systemic risks in the Union pursuant to Art. 34.1. **Art. 28**: Online protection of minors referring to **GDPR** terms (28.2). AI **Art. 14: Terms and conditions** 14.1 Providers of intermediary services shall include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions: any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review, as well as the rules of procedure of their internal complaint handling system. **Art. 27: Recommender system transparency** Providers of online platforms that use recommender systems should set out the terms and conditions (e.g. how data is used in algorithms, criteria). **Art. 34 & 35: Systemic Risk Assessment & Mitigation** Providers of VLOPs and of VLOSEs shall diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and related systems, including algorithmic systems, or from the use made of their services (34.1). They shall also put in place reasonable, proportionate and effective mitigation measures incorporating those for testing and adapting their algorithmic systems, including their recommender systems. **Art. 40.3**: Providers of VLOPs and VLOSEs shall explain the design, the logic, the functioning and the testing of their algorithmic systems, including their recommender systems.

Policy	References within
	Cybersecurity **Recital 108**: In addition to the crisis response mechanism for VLOPs and VLOSEs, the Commission may initiate the drawing up of voluntary crisis protocols to coordinate a rapid, collective and cross-border response in the online environment. Such can be the case, for example, where online platforms are misused for the rapid spread of illegal content or disinformation or where the need arises for rapid dissemination of reliable information. **Art. 34 & 35 again** **35.1(f)**: “reinforcing the internal processes, resources, testing, documentation, or supervision of any of their activities in particular as regards detection of systemic risk.” Cyber + AI + data **Art. 69: Power to conduct inspection** 69.2(d): the Commission may conduct all necessary inspections (VLOPs VLOSEs or any other legal person), ask to be provided with access to and explanations on its organisation, functioning, IT system, algorithms, data-handling and business practices and to record or document the explanations given.
Cyber Resilience Act (2024) Main domain: cyber Subsidiaries: artificial intelligence, data	Cybersecurity **Art. 1: Subject matter**: This regulation is about digital products cybersecurity throughout their lifecycle. **Art. 3.3: Definition of ‘cybersecurity’** means cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881 (Cybersecurity Act). **Art.13.3: Obligations of manufacturers The cybersecurity risk assessment** shall be documented and updated as appropriate, shall comprise at least an analysis of cybersecurity risks based on the intended purpose and reasonably foreseeable use, as well as the conditions of use, of the product with digital elements, taking into account the length of time the product is expected to be in use. **Art. 16: Establishment of a single reporting platform** Simplify the reporting obligations of manufacturers, a single reporting platform shall be established by ENISA. The day-to-day operations of that single reporting platform shall be managed and maintained by ENISA. The architecture of the single reporting platform shall enable Member States and ENISA to put in place their own electronic notification endpoints. → Report actively exploited vulnerabilities and incidents. **IMPORTANT: ANNEX I - Essential cybersecurity requirements** Lays out technical and organisational requirements, including protection against known vulnerabilities, authentication mechanisms, etc. Data **Art. 14.5 (a)**: An incident having an impact on the security of the product with digital elements shall be considered severe where it negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity, or confidentiality of sensitive or important data or functions. **Art. 53: Access to data and documentation** Where necessary to assess the conformity of products with digital elements and the processes put in place by their manufacturers with the essential cybersecurity requirements set out in Annex I, the market surveillance authorities shall, upon a reasoned request, be granted access to the data, in a language easily understood by them, required to assess the design, development, production and vulnerability handling of such products, including related internal documentation of the relevant economic operator. AI **Art. 12: High-risk AI systems**. Ensures the alignment between the Cyber Resilience Act and AI act. 12.2: For products with digital elements and cybersecurity requirements referred to in paragraph 1 of this Article, the relevant conformity assessment procedure provided for in Article 43 of Regulation (EU) 2024/1689 (AI Act) shall apply.
Cybersecurity Act (2019) Main domain: cyber Subsidiaries: data, artificial intelligence, quantum, (others)	Cybersecurity **Art. 3**: ENISA’s mandate. **Art. 8**: Market, cybersecurity certification, and standardisation. **Art. 46**: European cybersecurity certification framework. Data **Art. 41: Protection of personal data** **Art. 51: Security objectives of European cybersecurity certification schemes** include: (a): “to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process”. (b): ”to protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration, or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process”. (e): “to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom”. 51 (e).

Policy	References within
	AI **Art. 2: Subject matter and scope**. The CRA lays down (b) a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union. **Art. 51: Security objectives of European cybersecurity certification** (j) ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities and are provided with mechanisms for secure updates. Quantum **Art. 9: Knowledge and Information** stipulates that ENISA shall: (a) perform analyses of emerging technologies and provide topic-specific assessments on the expected societal, legal, economic and regulatory impact of technological innovations on cybersecurity. Supply chains Recital (11): Modern ICT products and systems often integrate and rely on one or more third-party technologies and components such as software modules, libraries or application programming interfaces. This reliance, which is referred to as a 'dependency', could pose additional cybersecurity risks as vulnerabilities found in third-party components could also affect the security of the ICT products, ICT services and ICT processes. **Art. 51: Security objectives of European cybersecurity certification schemes** (d) to identify and document known dependencies and vulnerabilities; (j) that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities and are provided with mechanisms for secure updates.
NIS2 Directive Main domain: cyber Subsidiaries: artificial intelligence, data	AI **Recital 51**: Encourages Member States to promote the use of innovative technologies, including AI, to enhance the detection and prevention of cyberattacks. The recital emphasises that such use should comply with data protection laws, including the data protection principles of data accuracy, data minimisation, fairness and transparency, and data security, such as state-of-the-art encryption. **Recital 89**: Essential and important entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine-learning systems to enhance their capabilities and the security of network and information systems. Data **Article 7.2 (h)**: National cybersecurity strategies should include relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between entities in accordance with Union law. **Article 10.7**: The CSIRTs may exchange relevant information with third countries' national computer security incident response teams, including personal data in accordance with Union data protection law. Supply chain **Recital 44**: The CSIRTs should have the ability, upon an essential or important entity's request, to monitor the entity's internet-facing assets, both on and off premises, in order to identify, understand and manage the entity's overall organisational risks as regards newly identified supply chain compromises or critical vulnerabilities. **Recitals 90**: To further address key supply chain risks and assist essential and important entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related risks. **Article 14.4 (i)**: The cooperation group should carry out coordinated security risk assessments of critical supply chains in accordance with Article 22.1. **Article 22.1**: The Cooperation Group, in cooperation with the Commission and ENISA, may carry out coordinated security risk assessments of specific critical ICT services, ICT systems or ICT products supply chains, taking into account technical and, where relevant, non-technical risk factors.

Finland

Name of strategy	References within
Space Strategy 2030 (2025) Main domain: space Subsidiaries: data, cyber	Data **P.13**: Data management, transmission for societal and security purposes: Highly accurate location or time data is essential for many of the key functions of society, and most of this data is produced by satellites. Remote sensing satellite systems observing the earth enable a continuous data flow for monitoring the environment and weather conditions, mapping natural resources, monitoring and anticipating disasters, and for the national and international security sector. Supply chain emphasis on security of supply: **P.13**: The information and services produced by space activities are part of societal resilience and they are extensively used to secure the infrastructures, services and functions important to security of supply. **P.19**: The risks arising from the supply chains used to provide space services must be identified and the continuity of these chains ensured. Potential disruptions to the services must be identified and prevented and the recovery process must be on a systematic basis. Cyber **P.15-16 NIS2 and CER**: Finland became a full member of the ESA in 1995, joined the EU SST partnership in 2023, and has pledged to maintain a national contact point and provide observation data for the partnership programme. For the space sector, the NIS2 and CER directives of the EU are relevant to the activities specified in the Act on Earth Stations. The EU Space Law initiative, one of the priorities of the Commission, is intended to supplement the NIS2 and CER directives and extend EU regulations to cover the space segment. **P.22**: The security of supply for society's critical infrastructure and functions will be strengthened by utilising space services. The dependence of terrestrial systems on satellite systems has been identified. The availability and continuity of the space services required for the critical functions of society has been secured. Resilience and cybersecurity of society will be strengthened.
6G Bridge program (2023) by Business Finland Main domain: connectivity Subsidiaries: data, cyber, AI, semi-conductors	AI **P.27**: 6G technology enablers and challenges: Smart AI/ML enabled networks and services. Networks and applications become intelligent, self-learning and context dependent; edge intelligence is the key technical enabler and challenges/complements centralised cloud solutions. **P.30**: Are identified as 6G strategic objectives: Mobile edge cloud; including, e.g. functionalities for improving RAN capabilities, near real-time AI solutions – small data approach. Distributed AI; distributed inference. Privacy preserving AI, Security of AI, software for highly distributed heterogenous massive networks of connected devices. Data + cyber **P.27**: 6G technology enablers and challenges: Data privacy and security. Expansion of verticals with new stakeholders and emergence of large number of new players providing different network elements, critical applications and operating different parts of networks sets new privacy & security requirements. Cyber **P.6**: The vision for 5G evolution and 6G is formed around three main pillars: performance, sustainability, and security/trustworthiness. **P.30**: Identified as a 6G strategic objective. 6G software: extremely distributed environment including e.g. software for highly distributed heterogenous massive networks of connected devices, software-based architecture solution evolutions for 6G architecture, trustworthiness and security of 6G software, virtualisation platforms, "agent"-based software solutions. **P.31**: Implementation challenges: The biggest fear related to 6G is the overall technology acceptance: if we cannot guarantee absolute security and privacy, the user will not trust 6G. Cyber + AI **P.29-30**: Identified as a 6G strategic objective: future networking technologies including e.g. 6G core and telecommunication cloud solutions, edge cloud solutions, AI driven networking solutions, end-to-end security/trust/dependability enablers, end-to-end resource optimisation and sustainability of mobile networks, new architecture solutions for radio access and core networks, secure backbone and Internet connectivity, automation and zero-touch of service and function orchestration and provisioning. Semiconductors **P.44**: Opportunities for devices and components including RF and antenna technologies, mmWave and THz solutions, baseband modems, hardware for security, cloud/edge/on-device AI processors, etc.

Name of strategy	References within
	Quantum **P.24**: 6G state-of-the-art and future outlook: Careful and critical focus is necessary to distinguish between generic far-reaching wireless enablers and 6G enablers to be commercialised within the next 10 years. Areas such as semantic communications or quantum communications go far beyond the 2030s, possibly beyond the 2040s. Even THz/sub-THz communications is a border line within the 6G timeframes. **P.42**: Are identified as 6G test bed enablers: Quantum communication technologies and solutions (2025-2026), utilisation of quantum computing in telecom system design and implementation (2027-2030).
Artificial Intelligence 4.0 programme (2022) Main domain: artificial intelligence Subsidiaries: data, quantum, cyber, semiconductors	Data **P.19**: One of the development priorities is boosting digital skills and speeding up the adoption of technologies accelerating twin transition in industrial SMEs. **P.23** Measure 7: Preparing a growth programme for the data economy. A growth programme will be launched to increase the utilisation of industrial data. Business Finland, or an alternative actor close to companies, will coordinate a programme in which companies, start-ups and research actors of different sizes join forces to speed up the creation of a responsible data economy in Finland. **P.24**: One of the development priorities is to make Finland an international frontrunner in twin transition. Finland will play a role in the drafting of European artificial intelligence, data and industrial strategies and measures, and should focus domestic inputs in an optimum manner. Quantum **P.12**: Identified as the most important key technologies for Finland: wireless networks, artificial intelligence, microelectronics and photonics, quantum technology, space technology, smart manufacturing. Quantum + Cybersecurity **P.26**: Measure 10: Strengthening Finland's position in transatlantic discussions on technology and trade policy matters. The following themes have been selected as spearheads of international impact in the Artificial Intelligence 4.0 programme: high-performance, edge and quantum computing, connectivity, sustainable artificial intelligence, cyber security competence. Semiconductors + Cybersecurity + Quantum **P.15-16**: Measure 2: Enhancing the impact of key technologies by creating a national RDI (Research, Development, and Innovation) agenda to accelerate twin transition. The agenda will lead to the launch and construction of key projects in microelectronics, network technology, robotics, the quantum sector, edge computing, and security technology.
Finland's cybersecurity strategy (2024) Main domain: cyber Subsidiaries: data, quantum, artificial intelligence, space, semiconductors	AI **P.29 5.2**: Preventing Cybercrime: The development of artificial intelligence is making cybercrime more targeted and impactful, and it will accordingly become increasingly important to recognise the impacts of artificial intelligence and other disruptive technologies on cybersecurity, and to develop ways of responding to them. Data **P.13 3.1**: Cyber domain incidents may also be caused by various physical threats, such as power supply disruptions, floods, earthquakes, other natural disasters or solar activity, and damage due to human error. These may also disrupt data connections or the functioning of information systems and subsequently threaten cybersecurity. Data + AI **P.17 4.1**: Hostile state-sponsored operations, cybercrime, denial-of-service attacks, data leaks, and various malware and other incidents have nevertheless also become more common in Finland. New data scamming approaches enabled by artificial intelligence are already threatening both cyberspace and the information environment. There is a threat of new serious impacts that will be even more far-reaching. Quantum + Data **P.26 5.1**: Aiming for self-sufficiency in cryptographic technology: The confidentiality, integrity and availability of nationally important data repositories under all circumstances is an important aspect of cyber resilience. Progress in quantum technology threatens to break modern encryption algorithms and compromise datasets that require national protection. One of Finland's strategic objectives is to be self-sufficient in critical cryptographic technologies and prepared for the quantum threat by the beginning of 2030. Data + Space **P.31 5.2**: Improving the resilience of terrestrial systems with space services: The availability of space services such as time and geospatial data, telecommunications, and remote sensing is important for the functioning of society. The cybersecurity of space systems is monitored as part of maintaining space-related situational awareness and should also be considered in the conditions for authorising space activities and in life cycle management of systems.

Name of strategy	References within
	Semiconductors **P.14 3.3**: Technological progress increases everyone's responsibility for cybersecurity: The causes of technological incidents include human error in software development and related supply chains, and intentional vulnerabilities, such as security backdoors that enable criminals and state-sponsored operators to access information systems. **P.16 3.7**: Highlighting the security of service and supply chains: Service and supply chains have become longer, more complex, and increasingly difficult to manage. Supply chain attacks hack into the information systems of an organisation through the services that it purchases, or through the hardware or software of its service providers. Actors that are critical for the functioning of society must therefore ensure the cybersecurity of their service providers and supply chains.
Finland's quantum strategy (2025) Main domain: quantum Subsidiaries: data, cyber, artificial intelligence, advanced semi-conductors	AI + Data **P.18**: The quantum software field is extensive and has synergies with traditional software expertise, including artificial intelligence development and high-performance computing **P.22**: EuroHPC's decision to locate the next-generation supercomputer (LUMI-AI) and the AI Factory in Kajaani, at CSC's data centre, strengthens Finland's position in the development of hybrid computing. LUMI AI Factory will include an efficient quantum computing platform, making it the world's leading computing infrastructure combining high-performance computing, artificial intelligence and quantum computing. **P.24**: The success of quantum computing depends on how efficiently software can use quantum hardware and enable efficient hybrid computing that combines quantum computing, high-performance computing and artificial intelligence. Strengthening cooperation between quantum computing experts and artificial intelligence researchers can speed up the development of Finnish quantum algorithm and software companies. **P.35**: Ensure access for companies, researchers and students to world-leading quantum machines based on different technologies and enable the development of hybrid computing that combines high-performance computing (HPC), artificial intelligence (AI) and quantum computing (QC). Cyber + Data **P.24**: The introduction of quantum-secure encryption technologies and the protection of critical data as a pioneer in the EU countries will increase Finland's reliability as a partner. Quantum-secure communications infrastructure enables the establishment of IT solutions that require such security in Finland, supports the processing of sensitive data in these systems, and facilitates the development and export of related hardware, software and service solutions. Cyber **P.28**: Safeguard national security and preparedness and to strengthen the defence industry base: Access to quantum infrastructure and computing strengthens the effectiveness of different sectors, such as enabling the timeliness and reliability of critical security and situational awareness services, in extreme weather situations for example. **P.30-31**: On risk management: Finland has moved towards quantum-secure encryption solutions and is prepared for the security challenges posed by quantum technologies in different sectors of society. The infrastructure essential for the critical functions of society has been protected and made quantum-safe. In the national security strategy, quantum technology is also identified as a transition technology that both improves national security and threatens it. **P.47**: The quantum infrastructure built in Finland is used to ensure security, for example, in testing or reverse engineering encryption solutions in accordance with the needs of both the authorities and critical actors in society. Semiconductors **P.6**: With microelectronics-based technologies, quantum sensing can be used, for example, in chip design and the quality assurance of production processes. **P.38**: On Competitive infrastructure to support the development of quantum hardware and components: Measure "Updating the shared RDI infrastructure for quantum devices and strengthening international competitiveness, using, for example, national research infrastructure funding and EURA-MET, the EU Chips Act and Quantum Act funding".

Name of strategy	References within
Chips from the North Semiconductor Strategy for Finland (2024) Main domain: semi-conductors Subsidiaries: quantum, data, cyber, artificial intelligence	Quantum **3.1**: "Finland can carve a niche in designing advanced chips and devices in lower-volume categories dependent on specialised expertise. There are opportunities for faster-than-average industry growth in emerging fields such as photonics, quantum technologies, new material R&D, and selected process technology niches for smaller countries to play an outsized role." **5.4**: Quantum is identified as one of the six growth "must-win" opportunities in the Finnish Semiconductor Vision: Focused efforts could reinforce Finland's competitiveness in these critical future technologies. **7.2.4.** and **7.2.6**: Examples of initiatives: SemiQon, which designs and produces silicon-based quantum processors; OtaNano, a national research infrastructure supporting research in quantum technologies and micro- and nanoelectronics; Kvanttinova, which pilots and develops facility for microelectronics and quantum technology; and IQM's manufacturing facility dedicated to the fabrication of superconducting quantum processors, including state-of-the-art equipment to manufacture multi-layer quantum chips as well as infrastructure for cryogenic characterisation. **7.2.5**: R&D collaboration: "The Chips from Finland initiative is focused on creating a European semiconductor and quantum industry ecosystem for local companies and researchers." Data + AI **5.2**: A growing need for sensors is driven by e.g. the need to supply data for AI systems with most devices collecting external data using MEMS/NEMS sensors. Although these sensors constitute a small part of the overall semiconductor demand, they are crucial for linking real-world data to computation. **7.1.2**: AI systems process vast volumes of data at high speeds, enabled by technologies such as photonics. The growing reliance on AI necessitates increased cloud computing capacity and data storage, which in turn depend on servers equipped with semiconductor chips. **7.2.5**: R&D collaboration: SoC HuB is a joint initiative supported by Tampere University and industry. It supports the design of new system on-chip solutions for 6G, artificial intelligence, imaging, and security applications. Data + cyber **3.1**: The growing need for performant data processing, data sensing and data storage capacity → growing demand for semiconductors. **7.1.2**: Semiconductors are integral to military systems and cybersecurity: Vulnerabilities in these components increase the risk of espionage and data theft. Secure supply chains are crucial for national security.

SITRA WORKING PAPER October 2025
Sitra working papers provide multidisciplinary information about developments affecting societal change. Working papers are part of Sitra's future-oriented work conducted by means of forecasting, research, projects, experiments and education.

ISBN 978-952-347-424-6 (PDF) www.sitra.fi

SITRA.FI
Itämerenkatu 11–13
PO Box 160
FI-00181 Helsinki
Finland
Tel: +358 294 618 991
in Sitra