Strategic orientation report
2025

4 Archetypes

for the digital function in 2040

Cigref
SUCCEED
WITH DIGITAL

4 Archetypes

of the digital function for 2040

Foreword

The digital world we inhabit presents both tremendous opportunities and complex challenges. Rapid technological innovation – ranging from generative artificial intelligence to quantum computing – is reshaping economies and transforming business models, while simultaneously challenging our societal equilibrium. This dynamic unfolds within a global context defined by geopolitical uncertainty and urgent environmental concerns. Consequently, traditional planning cycles are becoming increasingly difficult to execute. Faced with such uncertainty, the temptation is to navigate solely by sight – reacting to events rather than anticipating them. However, it is precisely when the horizon is obscured that a strategic compass becomes an indispensable asset for decision-makers. This is the primary objective of our Strategic Orientation Report: to provide our members and the wider ecosystem with insights and actionable strategies to collectively build a digital future of our choosing, rather than one imposed upon us.

Since 2020, this annual publication has systematically explored the major transformations impacting our organisations, analysing trends, disruptions, and potential long-term scenarios. Armed with this understanding of the external environment, we are shifting our focus this year. Our sixth Strategic Orientation Report addresses a more intimate yet equally fundamental question: the future of our digital departments. After mapping out the world to come, it is time to consider our own future. The challenge shifts from merely asking "What might happen?" to collectively defining "What do we aspire to become?". The core challenge lies in defining the strategic futures that digital leaders can embody to continue creating value for their organisations.

To fuel this ambition – and having updated the five areas of digital transformation that have guided our approach for the last six years – this report introduces a new framework. We have developed four "archetypes" of the digital function for 2040. These models of tomorrow's digital function are neither prescriptive nor descriptive; they are not organisational proposals. Rather, they provide a structured reasoning method to initiate a forward-looking evaluation of the digital function within large organisations. Each of these possible futures must be assessed against the specific dynamics of each organisation to determine its relevance and resilience. This approach enables us to identify levers for action, alliances to be forged, and avenues to be explored, allowing each Cigref member to chart their own course. The aim is to provide concrete guidelines to support the development of robust digital strategies over the next fifteen years.

The rigour of this forward-looking approach and the quality of its conclusions rely entirely on the mobilisation of our collective intelligence. I would like to thank the members of our Strategic Advisory Board – leaders and qualified individuals whose vision and experience ground our work in operational and strategic realities. I would also like to commend the commitment and valuable contribution of the Youth Strategic Advisory Board. Their perspective, digital culture, and boldness are fundamental in challenging our certainties and enriching our vision of the future for which their generation will be sustainable. We are also grateful to our partner Futuribles, whose methodological support and intellectual rigour have ensured the soundness of our thinking since this project began.

We entrusted the illustration of this demanding undertaking to Ixène, with whom we have collaborated several times to our great satisfaction. His drawings are much more than mere embellishments. With their wit, subtle humour, and ability to synthesise complex ideas into striking images, they offer a valuable perspective. This "design fiction" approach, combining in-depth analysis and visual creativity, reflects our belief that we must utilise all forms of intelligence to comprehend the future. This unconventional approach encourages us to take a step back and address serious subjects with composure, allowing us to be serious without taking ourselves too seriously.

This report is not merely an analysis; it is a call to action. The guidelines and recommendations set out herein have a clear objective: to build a sustainable digital world that is environmentally and economically sound, ethically and socially responsible, and trustworthy – safeguarding our security and ensuring data protection. Digital technology will drive the growth and competitiveness of our European businesses, offering resilience in the face of crises and acting as a pillar of cohesion in service of society and its democratic values.

On behalf of the Cigref Board of Directors and all the teams who contributed to this report, I hope you find it inspiring and that it forms the basis for your future actions.

Emmanuel Sardet, President of Cigref

Executive Summary

Partie 1 – Prospective analysis

This section presents a prospective study on the five major areas of digital transformation. *The objective is to encourage strategic thinking among Cigref members and the broader digital ecosystem through a series of in-depth scenarios and disruptive hypotheses. Below are the main themes.*

Field 01 – Digital Geopolitics

The geopolitical upheavals of 2025 have confirmed that digital technology has become a strategic battleground. Sino-American rivalry exerts significant influence on all technological issues, while Europe seeks to preserve its sovereignty amidst increasing dependence on American cloud and AI giants.
We are witnessing a growing trend where sovereign functions are delegated to private actors, blurring the boundaries between state power and economic influence. Cyberattacks are escalating, conflicts are shifting to the digital sphere, and national agencies are collaborating to counter the erosion of international law and institutions. The potential for the internet to fragment into regional blocs ("splintering") raises concerns about its universal nature.
In this context, digital resilience is becoming imperative: diversifying suppliers, controlling infrastructure, and anticipating disruptions are now major strategic priorities.

Field 02 – Digital Economy

The hegemonic position acquired by a small number of non-European digital players is widening the competitiveness gap across the Atlantic. The large-scale financial race led by these organisations to absorb strategic infrastructure strengthens existing market positions.
European initiatives are emerging to structure digital resilience through credible, large-scale technological alternatives. These aim to reduce direct dependence on US services – marked by rising prices – while stemming growing indirect pressure from Chinese mega-competitors.
In this fragmented landscape, digital trust based on global data control is becoming a strategic lever. Support from regional regulations – particularly European ones – is growing but still struggles to back a clear civilisational and industrial project, risking either superficial sovereignty or overly rigid regulation of innovation.

Field 03 – Technology & Innovation

Global digital infrastructures, particularly cloud infrastructures, rely more than ever on three essential pillars: computing power, storage capacity, and network effect. Optimising these has become a strategic issue, both to support the rise of AI and to ensure the resilience of critical systems. The transition toward leaner, more interoperable, and secure architectures is accelerating.

Artificial intelligence is transforming economic models, organisations, and the social order as a whole. On the one hand, agentic AI models (capable of autonomous action) herald a profound redefinition of use cases in sectors as varied as health, energy, finance, and defence. On the other hand, the growing importance of these technologies makes AI a diplomatic, industrial, and strategic lever, with major implications for technological sovereignty and digital security.

These developments are accompanied by a renewed global race for infrastructure, data governance, and risk minimisation. Simultaneously, quantum and space technologies are establishing themselves as critical layers of tomorrow's digital infrastructure; immersive interfaces are poised to change how we interact with reality; and secure collaborative platforms are becoming essential prerequisites.

These transformations require greater coordination between public and private actors to define the intended purpose of these tools, anticipate potential applications, manage major risks, and ensure ethical and resilient governance of information systems.

Field 04 – Digital Responsibility

In a context of digital expansion, the responsibility of sector players to control their environmental impact is becoming increasingly significant.

The demand for raw materials to manufacture equipment and deploy digital infrastructure is growing. Simultaneously, the industry must contend with limited water availability due to water stress and stricter regulations. Furthermore, the digital sector contributes significantly to rising energy consumption and global greenhouse gas emissions. The increase in extreme weather events also contributes to the fragility of digital infrastructure, potentially undermining its insurability.

At the same time, practices aimed at reducing energy and resource consumption are becoming widespread, and the potential of digital technology to maximise energy efficiency is increasingly exploited. In response, the European Union is implementing incentives and regulations to limit the sector's environmental impact, unlike other less prescriptive powers. R&D is also advancing to design more sustainable electronic materials and improve the energy performance of technologies.

Field 05 – Digital & Society

Digital technology has enabled daily life in both private and professional spheres. In the workplace, the development of digital uses is accelerating, particularly with the widespread dissemination of generative AI. These developments occur against a backdrop of an ageing workforce and the diversification of workers' skills. Simultaneously, digital technology is becoming ubiquitous in everyday life. This creates a digital divide likely to widen further with rapid AI progress.
Digital technologies have and will continue to have ambivalent impacts on individuals and lifestyles. On the one hand, they can facilitate the management of tedious and unproductive tasks (particularly in the workplace), but also facilitate access to personalised services. On the other hand, they can have negative impacts on health, employment and cyber risks, which organisations and individuals are increasingly ill-equipped to deal with.

Part 2 – Archetypes of the digital function of the future

***This second part explores possible futures for digital development by 2040**. It proposes a typology structured around four archetypes, designed as a basis for reflection to enable organisations to prepare effectively. Beyond analysing the prospective context ("What could happen?"), this section invites a retrospective reflection on the future of digital management itself ("What could it become?"). These archetypes are neither normative models nor exclusive scenarios; they do not represent any specific organisation.*

1. The Lab
Positioned at the heart of strategy and innovation, The Lab embodies a highly integrated and visible digital function. It acts as a lever for competitiveness and influence within its ecosystem (Executive Committee, peers, public policy, industrial standards). With multi-year innovation budgets, it forges strategic partnerships with governments and consortia. Its organisation is global and decentralised, supported by a high degree of AI automation. Above all, The Lab seeks strategic autonomy in an unstable geopolitical environment, while assuming a significant environmental footprint.

2. The Chameleon
An agile and responsive digital function, The Chameleon is results-oriented and operates in an unstable technological environment. It focuses on rapid transformation and actionable deliverables to meet business needs. Its organisation is flexible and distributed, with a strong ability to initiate or halt projects based on priorities. SaaS adoption is widespread, balanced by multi-cloud projects to ensure reversibility. AI streamlines processes, and environmental issues are integrated in a utilitarian manner rather than structuring the strategy.

3. The Stewards
In a context of regulatory pressure and environmental dependencies, the Stewards makes sustainability a key strategic criterion. It acts as a catalyst for sustainable innovation, serving the business lines and, where possible, external customers.
Its "Green IT-as-a-Service" approach combines operational performance with digital sobriety. Investments target low-carbon solutions, and governance is based on co-construction with stakeholders. The organisation is hybrid and decentralised, comprising technical, environmental, and regulatory profiles. AI and cloud are used with reason, contributing to the common good.

4. The Resourceful
Marked by geopolitical tensions, cyber risks, and budget restrictions, the Resourceful thrives by optimising constraints. It prioritises robustness, operational resilience, and business continuity. Its model relies on strong centralisation, valuing the human factor and technical expertise. Investments are geared towards securing critical infrastructure with low exposure to disruptive innovation. AI is used sparingly, cloud adoption is selective, and environmental issues are integrated pragmatically.

Part 3 – Principles of strategic action

***This last section focuses on ten principles for action**, identified to move from prospective research to concrete implementation, by projecting trends to the year 2040 and constructing archetypes of the digital function of the future. These elements aim to help organisations, and particularly their digital departments, prepare for the transformations to come.*

1. Proactive resilience - "Proactive resilience will become an asset in ensuring service continuity in the face of international crises."

2. Strategic autonomy policy - "The politicisation of digital activities, whether imposed or voluntary, will make it necessary to clearly define an internal policy of strategic autonomy."

3. Rebalancing value chains - "The increasing regionalisation of infrastructure, standards and regulations will require a de facto rebalancing of value chains."

4. Contractual flexibility - "Contractual flexibility will be a key factor in reducing technological dependencies."

5. Mastery of AI technologies - "Mastery of the various components of AI technologies will become an operational requirement."

6. Ecosystem-building capacity - "The ability to build ecosystems will become an essential lever for guiding and supporting technological innovation."

7. Anticipation of resource trade-offs - "Public-private dialogue on virtuous French and European regulations will become a key factor in the digital environmental resilience of organisations."

8. Environmental resilience of business models - "Energy optimisation and the use of more sustainable materials in the digital sector will be an integral part of business models."

9. Reasonable use of AI technologies - "Guidance and support for the reasonable use of AI technologies will become essential to making human-machine complementarity a source of sustainable organisational performance."

10. Enhancing digital skills - "The ability of organisations to anticipate digital skills needs and structure agile training programmes will become a key driver of organisational resilience."

Table of contents

Background note

Dated 4 September 2025.

« The future brings us nothing, gives us nothing; it is we who must give it everything to build it, give it our very lives. »

Simone Weil – L'enracinement.

Keeping with our annual tradition, Cigref's 2025 Strategic Orientation Report begins with a background note. The goal remains the same: to provide a clear and objective overview of the geopolitical, economic, and technological dynamics shaping our environment today. This description is naturally partial and does not claim to cover everything.

Our perspective is not neutral. It is that of a European observer who observes and analyses a world whose balance is changing at an unprecedented rate. The purpose of this note is therefore, with all due caution, to provide today's readers, and even more so tomorrow's, with some keys to understanding the global context as we perceive it in the summer of 2025, in order to shed light on the forward-looking assumptions and strategic directions we propose in this report.

While 2024 was marked by uncertainty, the summer of 2025 appears to be one of consequences. The uncertainty surrounding major political questions has cleared, giving way to a fractured landscape marked by profound disruptions in the global commercial and strategic order. The logic of blocs, the spread of protectionist policies and the questioning of multilateral frameworks are no longer working hypotheses but rather the input data for a new equation for all economic and geopolitical actors.

It is against this backdrop of accelerating fragmentation, where adaptability has become the most important strategic skill, that this note will attempt to identify the key trends shaping the present day. The aim is to understand the implications of this new world order in order to better prepare for it, without fatalism, of course, but with the realism that the current period demands.

For the past year, the world has been undergoing a major reshuffle.

Since the summer of 2024, events have unfolded at such a pace and with such intensity that there can be little doubt about the new configurations of the contemporary world. For Europe, and particularly for France, this sequence of events is not simply a continuation of past trends, but represents a break with the past. What we are experiencing is akin to an epoch-making shift, with a sudden transformation of the international balance of power, the contours of which remain unclear but the effects of which are already tangible.

Donald Trump's election as President of the United States in November 2024, followed by his return to the White House in January 2025, confirmed this feeling of radical change. More than just a shift in American foreign policy, this return marks the deliberate abandonment of the principles that had structured the world order since 1945. The new administration very quickly implemented a strategy to accelerate the US's disengagement from multilateral institutions. **The message is clear: the era of common rules is over**. The global economy is entering an era of brutal power struggles and bilateral negotiations dominated by immediate interests and power asymmetries, in which **every country, including historical allies, must defend its position in an environment that is now unstable and unpredictable.**

Strategically, this logic translates into a profound questioning of traditional alliances. The United States' commitment to NATO is no longer based on a shared vision of transatlantic security, but on a strictly transactional approach. European security is becoming a European affair. This long-feared disengagement, which began during Obama's presidency when he initiated the US pivot to the Indo-Pacific, has found its most spectacular manifestation in Ukraine. The drastic reduction in US military and financial support is upsetting the balance of power on the ground. Europe finds itself brutally exposed, forced to shoulder the economic, logistical and military burden of a high-intensity conflict on its doorstep, without yet having the concrete means or political cohesion necessary for such an effort, while the United States intends to retain exclusive political control over its confrontation with Russia.

For the European Union, this shock has been a wake-up call. The concept of strategic autonomy, often invoked but rarely implemented, has suddenly changed in nature. What was until recently mere rhetoric has become an imperative. The Union is discovering, often with astonishment, the extent of its dependencies. Faced with an America that has become unpredictable once again, a methodically expansionist China, strengthened by its industrial hegemony, and a cynical and unapologetic Russia that no longer hesitates to use brute force on Europe's borders, the question is no longer whether to become a power, but how, and how quickly. The entire architecture of European power is being called into question: defence, of course, but also industry, energy, trade policy, technology, security of supply and democratic resilience.

In this urgent context, France finds itself in a unique position. Historically driven by a desire for strategic independence for Europe, it is seeing its vision gain legitimacy and support among its partners. What French diplomacy has been advocating for several decades, mostly met with indifference and sometimes scepticism or even hostility, suddenly appears to be a necessity to the majority. But this potentially central position comes with a double challenge. Internally, the political and budgetary context limits France's ability to lead and undermines its voice and credibility. Externally, persistent divisions within the continent, diverse strategic cultures, divergent interests and national caution are slowing down any momentum for rapid integration of power policies.

The tariff war as a new paradigm in international relations.

The year 2025 will go down as a major turning point in the contemporary history of international trade. Reversing decades of liberal globalisation, the United States began the year with an aggressive trade strategy, marking a break with the multilateral framework inherited from the post-Cold War era. Under the guise of restoring supposed trade fairness, the US administration has implemented a series of protectionist measures on a scale not seen since the 1930s, brutally upsetting the balance of world trade.

In February 2025, a series of decrees introduced **dramatic increases in customs duties** on a wide range of imported products. Their closest partners, Canada and Mexico, were the first to be targeted, with 25% surcharges applied to almost all of their exports to the United States. Shortly afterwards, China found itself in the firing line, facing a rapid rise in tariff barriers: an initial 10% increase in March, followed by a punitive tax peaking at 104% in April on many strategic products. This policy was then extended, affecting more than 70 countries and bringing the average US tariff rate to nearly 29%, an all-time high since the establishment of the modern trading system and unprecedented since the early 20th century.

In the United States, the economic effects of this tariff war are fuelling ongoing controversy. The White House highlights tens of billions of dollars in tax revenue generated by the Treasury and the partial relocation of certain value chains. However, macroeconomic indicators paint a more nuanced picture. Inflation in the United States, fuelled by rising import costs, reached 2.6% in June 2025, causing concern in the markets. At the same time, growth is slowing and is expected to peak at 1% in the second half of 2025, according to the most optimistic projections. Several studies agree that the burden of these new tariffs is largely being passed on to the end consumer, weakening domestic demand.

On a global scale, the repercussions are clearly negative. By disrupting supply chains that have been established for decades, the new American trade policy is forcing companies to rapidly reconfigure their supply networks. Asia, which is heavily integrated into trade flows with the United States, is paying a heavy price, while the European Union is facing increasing tariff pressure. This rise in trade tensions is part of a general climate of instability, where economic certainties are giving way to shifting geopolitical calculations. Investors, faced with a deteriorating legal environment, are reviewing their strategies in a context of eroding predictability in commercial law.

Sino-American relations, already marked by several years of trade rivalry, escalated further in the spring. In response to the massive tariffs imposed by Washington, Beijing adopted equivalent retaliatory measures, including taxes of up to 84% on certain American products and restrictions on technology exports. At the same time, China has strengthened its international stance, presenting itself as a pillar of stability and solidarity for emerging countries affected by the unpredictability of US trade policy. This clear desire to position itself as a sustainable alternative contrasts with the confrontational approach adopted by the United States.

However, faced with the risk of a total breakdown, a **relative de-escalation** took place in May, following closed-door negotiations in Switzerland. A temporary agreement allowed for the partial suspension of the most extreme measures: US customs duties were reduced from 145% to 30%, while China reduced its own tariffs to 10%. This fragile truce does not erase the deep structural mistrust between the two powers. Rather, it highlights the constant alternation between heightened rivalry and the search for pragmatic coexistence, reflecting what is now a permanent balance of power.

In this tense context, the European Union sought to avoid a head-on confrontation with Washington. A bilateral agreement was reached on 27 July 2025, sealing a compromise that was considered imperfect, even unfair. The EU agreed to a 15% tax on most of its exports of goods to the United States, while sparing a few sensitive sectors. In exchange, it committed to a massive investment effort, announced at $600 billion on American soil, to purchases of gas and oil worth $750 billion over the next three years, while suspending any retaliatory measures for a period of six months. While this arrangement has prevented an immediate escalation, it is perceived in Europe as a strategic setback, wrested from Ursula von der Leyen under pressure from Donald Trump. Criticism was quick to emerge. Several European officials have denounced a flagrant imbalance in the terms of the agreement, highlighting the lack of meaningful reciprocity and the potential impact on European industry. This compromise, seen as a default choice, illustrates the EU's weakness in the face of an increasingly unapologetic American strategy.

From Washington's point of view, this agreement represents a diplomatic victory. It confirms an unprecedented and unbalanced tariff level, neutralises European retaliation in the short term and brings new financial flows to the US economy. In the eyes of its promoters, it validates the relevance of a policy of confrontation, which aims less to restore the trade balance between Europe and the United States than to redraw the balance of power on a global scale.

This development has been accompanied by a sharp weakening of the World Trade Organisation. Although the United States has not officially announced its withdrawal, its suspension of financial contributions in 2024 and 2025, and the submission to Congress of a resolution to denounce the WTO's founding agreement, reflect a profound disengagement. Already weakened by the US blockade of its dispute settlement body and undermined by the lack of support from its main founding power, the WTO finds itself reduced in its capacity to act. This de facto disengagement by the United States confirms the questioning of the multilateral trade order as it was conceived in the 1990s. In practice, the global trading system is shifting towards a fragmented model, dominated by a proliferation of bilateral and regional agreements. While some economic powers such as the European Union, China and Japan are striving to preserve shared legal frameworks, their effectiveness remains relative in the absence of a fully legitimate central authority. This institutional vacuum is fuelling a drift towards a world where rules are dictated by force, where negotiation replaces law, and where uncertainty becomes the norm. Several economists are already talking about "trade anarchy", characterised by chronic instability, increased distortions and widespread exposure to geopolitical shocks.

Thus, the tariff war of 2025 cannot be reduced to a temporary crisis or a simple fluctuation in customs policies. It embodies a lasting shift towards a world where bloc logic, the defence of national interests and power tactics prevail over openness, cooperation and predictability. **This new paradigm, still in its infancy, heralds a structural reshaping of international relations, against a backdrop of strategic instability that is set to intensify in the coming years**.

Ukraine, Gaza: Seeking a necessary yet distant peace.

In the middle of summer 2025, the conflicts in Ukraine and Gaza remain at the centre of international relations. Far from abating, they illustrate with particular acuity the brutalisation of power relations and the exhaustion of the conflict resolution models inherited from the 20th century. Each, in its own way, acts as a powerful indicator of the new divisions in the world.

On Ukraine

On the ground, the war in Ukraine continues without any real strategic shift. The Russian army, confident in its superiority, has stepped up its pressure in Donbas and the Kharkiv region, pursuing a war of attrition that is gradually wearing down Ukrainian forces. Despite the courage of its people and the mobilisation of its last reserves, Ukraine is struggling to compensate for the relative decline in US military aid, while European efforts, although real, remain fragmented. In this asymmetrical balance of power, Moscow seems to favour a long-term strategy, betting on the economic and political exhaustion of Kyiv and its allies. Ukrainian society, for its part, remains largely determined to refuse any territorial concessions, even at the cost of a prolonged conflict, aware that any capitulation would pave the way for further aggression. Europe, for its part, is gradually finding itself on the front line of a confrontation that goes beyond the Ukrainian question alone and threatens the security balance of the European continent as a whole.

On the diplomatic front, the dynamics of the negotiations illustrate this shift in the balance of power. The summit between Trump and Putin in Alaska on 15 August 2025 spectacularly showcased the diplomatic rehabilitation of the Kremlin leader, who is still subject to an international arrest warrant, without the United States obtaining any concessions from him. With no ceasefire and an invitation to a future summit in Moscow, this nearly three-hour meeting between the two leaders raised more questions than it answered. The meeting organised in Washington the following Monday between Trump and Ukrainian President Volodymyr Zelensky, in the presence of key European leaders, confirmed the American President's desire to disengage from a conflict he considers costly and secondary, and his intention to favour a transactional approach marked by economic and political concessions demanded of his allies. Vladimir Putin, a skilled tactician, exploited this stance to obtain symbolic concessions, while maintaining maximalist demands that were unacceptable to Kiev, such as recognition of the annexation of Crimea, lasting control of the occupied territories, the absence of Western troops on Ukrainian soil, and NATO's definitive commitment to reject any request for Ukraine's membership. The European Union, caught between American impatience and Russian brutality, is trying to maintain strategic consistency, based on three principles: first, the rejection of any peace "imposed" on Ukraine; second, the mobilisation of its financial resources to support Ukraine's efforts; and third, the outline of autonomous European security guarantees. But the balance remains fragile. European diplomacy has understood that Donald Trump must be treated as an unpredictable and narcissistic actor, while remaining convinced that only peace based on law and not on force can bring lasting stability to the continent. This conviction, however, could soon be dissolved in the acid bath of realpolitik, a bath that old Europe has filled itself with its structural geopolitical weakness, and into which it is being brutally pushed by what will undoubtedly appear to be a circumstantial American-Russian collusion.

On Gaza

In the Middle East, the conflict that began in Gaza has shifted from open warfare to a severe humanitarian and security crisis. On the ground, this control strategy was formalised in August 2025 by the Israeli security cabinet's decision to establish a permanent occupation of the northern part of the Gaza Strip, officially to create a "buffer zone" and prevent any resurgence of the organised military threat from Hamas. The situation has therefore become entrenched in a low-intensity conflict, marked by targeted operations and sporadic outbreaks of violence. For the people of Gaza, this new reality is compounded by an unprecedented humanitarian catastrophe, where the destruction of infrastructure and the blockade of aid have created a situation of social collapse and endemic famine. The announced reconstruction of the Gaza Strip remains a distant prospect, if not a fiction, leaving the territory in a total impasse, suspended between a war that dare not speak its name and a peace that is clearly unlikely.

On the diplomatic front, this crisis seems to have served as a catalyst for a strategic repositioning by the United States. Breaking definitively with the two-state solution paradigm, which several Western leaders are nevertheless attempting to revive at the UN, notably on the initiative of President Macron, the Trump administration has favoured an approach to regional stabilisation based on strengthening the Abraham Accords and forming a security alliance against Iran and its nuclear programme. In this new architecture, the Palestinian question is deliberately marginalised, reduced to the status of a humanitarian problem to be contained. Regional powers, such as Turkey and the Gulf monarchies, are navigating this diplomatic vacuum to advance their own interests, while Iran continues to exploit the Palestinian cause to fuel instability despite the military neutralisation of most of its proxies in the Near and Middle East. The European Union, for its part, is seeing its role as mediator and main donor erode to the point of insignificance. Its diplomatic approach, based on international law and the search for a political solution, has become inaudible in an area where dialogue seems to have been definitively eclipsed by the cynical management of power relations. The Palestinian tragedy, devoid of any political horizon, now appears to be nothing more than an adjustment variable in a regional equation that is beyond its control.

What about China ?

Amidst the turmoil of the world's new disorders, China remains a mystery, not in the sense that we do not understand it, but in the sense that we seem never to have finished understanding it.

Faced with Washington's strategy of chaos, Beijing is deploying a remarkably consistent long-term diplomatic approach, in which each crisis is seen as an opportunity. While Xi Jinping's China still aspires to position itself as the champion of an alternative world order, more favourable to autocracies and the interests of the "Global South", its trajectory is far from linear. The most striking illustration of this is the BRICS summit in Rio on 6 and 7 July. Xi Jinping's notable absence, the first in more than ten years, revealed the fractures that now run through this enlarged bloc, which is subject to both American pressure and internal differences among its members. This episode suggests a diplomatic adjustment by Beijing which, faced with a multilateralism that is less controllable than before, seems to favour bilateral formats and more controlled forums to weave its web of influence.

Domestically, this external confrontation serves to consolidate power. The reinforcement of nationalist rhetoric and the focus on "total national security" justify increasingly intrusive social and technological control, consolidating a system of which Xi Jinping appears to be both the architect and the absolute guardian. The Taiwan issue remains the main red line, maintained in a calculated strategic ambiguity that alternates between demonstrations of military force, as seen last spring, and calls for "peaceful reunification". This oscillation keeps the international community in uncertainty about an initiative whose timing and terms are unpredictable.

However, cracks are appearing beneath the veneer of power of this geopolitical colossus. Far from the miracle of previous decades, the Chinese economy seems to have entered an era of "stunted growth" that official statistics, whose credibility is increasingly being questioned, are struggling to conceal. Chinese growth slowed in July 2025, and economists increasingly doubt that the government's official targets, notably 5% growth in 2025, will be met. The country certainly retains a dominant position in strategic sectors such as electric batteries, electric vehicles, solar energy, rare earths and telecoms infrastructure, but it is struggling to rebalance its model towards more robust domestic consumption. The property crisis, which has never really been resolved, continues to undermine household confidence, as highlighted in February by the bankruptcy of property developer Vanke, while youth unemployment has reached worrying levels in major cities. The trade war triggered by the United States, despite a partial de-escalation, is weighing on exports and accelerating the quest for technological self-sufficiency, at the cost of colossal investments whose benefits remain uncertain. This dynamic is ambivalent for Europe, which is under pressure from fierce competition in many industrial sectors, while at the same time seeing opportunities for diversification, protection of its own industries and affirmation of its strategic autonomy. In this unstable balance, however, Beijing retains considerable room for manoeuvre, thanks to the discipline of its state apparatus, the centralisation of its resources and its unrivalled capacity for fiscal and financial intervention. But despite its manufacturing performance and its move upmarket, the future of the Chinese economic model remains fraught with uncertainty, in a worrying context of statistical and political opacity.

More profoundly, it is the human foundation of Chinese power that appears to be weakened and seems to be cracking. The long-predicted demographic winter is now a reality, its effects manifesting themselves with unprecedented brutality. Data from 2024 confirmed a third consecutive year of population decline, a trend that could accelerate in 2025. This phenomenon is no longer a statistical abstraction, but a social crisis that is spreading throughout all strata of society. It is reflected in growing pressure on a still-embryonic pension system, a labour shortage that is driving up production costs and, above all, growing collective anxiety about the future. The implicit social contract, based on continued prosperity in exchange for restrictions on political freedoms, could be fracturing, weakening the very foundations of the regime. The phenomenon of tang ping, literally "lying flat", a silent form of dissent among young people who reject marriage, procreation and consumerism, has been the most visible expression of this in recent years. The Communist Party is attempting to respond with more coercive pro-natalist policies and intensified propaganda, but these remedies seem futile in the face of a profound cultural shift that is eroding the very foundations of the "Chinese dream".

Europe, a sick continent.

Thus, the triptych of the United States, Russia and China outlines a world that has entered an era of systemic competition, where power relations have replaced multilateral frameworks. America has become unpredictable and transactional, Russia has settled into a posture of lasting conflict, and China, despite its internal fragilities, is methodically pursuing the construction of an alternative order. For the European continent, this new world order is not only an external challenge; it acts as a mirror, reflecting back the image of its own dependencies, divisions and the urgent need to define its place in this new equation.

The shock of American disengagement and the brutality of crises on its doorstep have transformed the concept of strategic autonomy from a mere rhetorical ambition to an imperative for survival. But between awareness and the capacity for action, the road ahead remains long. It is therefore against this global backdrop, both threatening and full of opportunity, that we must now examine Europe's strengths and weaknesses, and the unique place that France can, or could, occupy within it.

Donald Trump's arrival in the White House and the geopolitical tsunami of winter 2025 acted as a shockwave of rare violence on the European Union, forcing it to wake up abruptly after decades of strategic comfort under the American umbrella. American attempts to drastically reduce support for Ukraine and Washington's transactional approach to NATO shattered any remaining illusions of an unconditional alliance. Suddenly, strategic autonomy, long perceived as a French ambition inherited from Gaullism, became the watchword of a continent-wide debate marked by concern. This realisation, although now widely shared, nevertheless struggles to mask the disorder of the responses to it. In Berlin, the new Chancellor Friedrich Merz, although a fervent Atlanticist, has had to resign himself to a forced conversion to realism, accelerating German rearmament to unprecedented levels that were unimaginable just a year ago. In the East, a sense of abandonment has prompted Poland and the Baltic States to call for a credible European defence, without however abandoning their suspicion of Franco-German hegemonic ambitions. In the middle, Ursula von der Leyen's Commission is striving to play a bridging role, pushing for joint initiatives on armament, but constantly coming up against national interests and the diversity of strategic cultures that fragment the continent.

This political fragmentation is compounded by an economic and industrial crisis that lays bare the vulnerabilities of the European model. The trade agreement secured by Donald Trump last July is seen not only as a strategic setback, but also as a diktat that weighs heavily on an already sluggish economy. Caught between American protectionism and Chinese overcapacity, the European Union is seeing its economic competitiveness erode, in a context where, following the Leča and Draghi reports published in 2024, no one within its institutions can ignore what needs to be done in this area. There is intense debate between those in favour of maintaining openness, led by Germany, which is concerned about its exports, and those who are calling for tougher reciprocity. In this complex game, some European capitals are adopting an ambiguous stance, tempted to negotiate parallel bilateral agreements with Washington to protect their national interests, at the risk of further fracturing an already fragile European common front. This tension is paralysing any large-scale joint response, even though the investment needs in defence, energy transition and digital technology are colossal. In this context, nationalist temptations are reviving, with some Central European governments using the crisis to justify their withdrawal and criticise a Commission they consider too interventionist, effectively paralysing a European budget in which every euro is fiercely contested and which ultimately appears derisory in the face of the challenges.

It is in this turbulent landscape that France finds itself in the most paradoxical of situations. Never has its vision of a powerful Europe seemed so relevant and so widely shared out of necessity; but rarely has France seemed so constrained in its ability to embody it. The presidential discourse on European sovereignty is finding new resonance among partners who were previously sceptical, but it is coming up against a domestic reality that is undermining its impact. The government, engaged in a painful effort to restore public finances in order to contain an abysmal deficit, is struggling to find the budgetary leeway necessary to translate its ambition into action at the European level and enable the President of the Republic to embody the leadership needed to rally the heads of state and government of the European Union member states. Indeed, the credibility of a France that calls on Europe to make massive investments while itself being under the close scrutiny of the financial markets is constantly being questioned. Paris certainly has the diplomatic vision and, to a certain extent, the military tools, particularly with nuclear deterrence, but its voice is weakened by its own fragilities, leaving it in an uncomfortable position, that of a conductor with a respected baton, but whose authority is undermined by its own difficulties in keeping time and following the score.

France therefore faces an immense task. It must catalyse European awareness, while translating this awareness into concrete actions and sustainable institutions. It must transform a political intuition into a collective project and convince others that European sovereignty is not just a slogan, but an existential requirement for our continent. This requires political leadership, diplomatic consistency, sustained budgetary effort and community education on a continental scale. There is no certainty about Europe's ability to overcome its inertia or the coherence of its collective responses. But the alternative is now clear: assert itself or suffer, wake up or decline.

Finally, as we finalise this report, and following the announcements made by Prime Minister François Bayrou, who will hold the Government accountable before a National Assembly where he does not have a majority, on 8 September 2025, the possibility that France will end 2025 once again without a government or a budget cannot be ruled out. Such a scenario would plunge the country into a major political, economic and social crisis, with little prospect of a positive outcome before the 2027 presidential election.

In the blind spots of geopolitics.

The turmoil in the world caused by the reversal of American policy, ongoing high-intensity wars and Sino-American rivalry is the focus of attention. However, **this deafening noise risks masking other, quieter but equally significant transformations that are reshaping the global balance of power**. In the blind spots of current affairs, the Global South, Africa and the climate crisis are following trajectories that Europe cannot ignore.

The Global South, first of all, is taking advantage of the fragmentation of the world to assert itself. Far from forming a homogeneous bloc, its leaders, such as India, Brazil and Indonesia, practise pragmatic "multi-alignment", refusing to choose sides in order to better negotiate their interests with all the powers. This non-alignment is less ideological than transactional, much like "Trumpism". We are cautiously observing the winding paths of Narendra Modi, who is strategically moving closer to Washington to contain China while maintaining his ties with Moscow, and Lula, who is using Brazil's agricultural and environmental weight to engage in dialogue with both Europe and Beijing, while harbouring growing mistrust of Trump's United States.

For Europe, this complex game makes diplomacy more difficult. It is no longer possible to address a unified whole, and it must deal with a myriad of actors with divergent interests, who demand massive investments from Europe to counter Chinese influence and challenge the legitimacy of a Western order that they seek to reform to their advantage.

Africa, meanwhile, illustrates a cruel paradox. Largely absent from the headlines, except when violence erupts, it remains a theatre of deep crises and a major strategic issue for Europe. In the Sahel, security instability has worsened, creating lawless areas where trafficking thrives and predatory external actors extend their influence. The humanitarian situation in countries such as Sudan and the DRC has reached catastrophic levels, with risks of regional destabilisation. At the same time, the continent is experiencing unparalleled demographic and urban dynamism, and hubs of innovation are emerging despite colossal investment needs. For Europe, Africa is not a peripheral issue: it is a direct challenge on its doorstep, combining security imperatives, migration issues, competition for influence and the need to rethink economic partnerships that have fallen into disuse, going beyond simple development aid.

Finally, the climate crisis continues to accelerate, indifferent to political agendas. Geopolitical upheavals have relegated the ecological emergency to the background, creating a vicious circle in which the focus on short-term energy security and increased defence budgets comes at the expense of investment in environmental transitions. The summer of 2025, with its new temperature records and extreme events, served as a reminder that the planet's calendar does not match that of government offices. The new stance of the US administration and the priority given to the security of fossil fuel supplies in Europe are hampering global cooperation, making the 1.5°C target virtually unattainable. The climate crisis is no longer a distant threat. It is now, unfortunately, a time bomb under the global economic and political edifice, a factor of instability that will exacerbate tensions over resources, particularly water, migration flows and the viability of entire sections of the global economy.

Thus, the overall picture for the summer of 2025 is that of a world that has entered an era of systemic competition, where power relations have replaced multilateral frameworks. However, this observation of fragmentation should not obscure the many dynamics of resilience which, although discreet, demonstrate resistance to the inevitability of decline. These positive signs exist, whether through the emergence of effective regional diplomacy, as illustrated by Brazil's successful mediation in the crisis between Venezuela and Guyana, or through the persistence of technical multilateralism capable of delivering tangible results, such as the new treaty on pandemics, concluded under the auspices of the WHO, with the participation of the United States. While these signals are not enough to reverse the overall trend, they remind us that history is not yet written, that there is still room for action and cooperation, and that glimmers of hope continue to shine, even in these times that may seem very dark to our generation.

Digital technology in the age of AI, critical infrastructure and resilience.

It is against this global backdrop, which is both threatening and ambivalent, that we must now examine the technological and digital sphere, which is also subject to the same dynamics of confrontation and the quest for autonomy.

Artificial intelligence: between competitiveness and speculative bubble

Over the past year, and particularly since Donald Trump took office in the White House, we have seen **an unprecedented acceleration in investment in data centres**. The dual race for technological hegemony in artificial intelligence and for control of a hypothetical
"general super intelligence" has triggered an explosion in investment. Computing power is becoming one of the most coveted strategic resources. This new gold rush is fuelled by American tech giants and supported by an administration that has reaffirmed that technological hegemony is one of the main pillars of its power policy. It is materialising in the form of a proliferation of data centres, whose size and energy consumption are growing exponentially.

This frenzy is reminiscent of the euphoria that preceded the bursting of the dot-com bubble in the early 2000s. The debate over a **potential "AI bubble"** has spread from expert circles to the heart of economic news. Major figures in the sector, such as OpenAI CEO Sam Altman, are now openly drawing parallels with the dot-com bubble, expressing concern about the growing gap between stratospheric valuations and actual revenue generation. While some analysts qualify this view by pointing to the very real profits and cash flows of a few titans such as Nvidia, numerous studies confirm that the majority of companies investing heavily in AI are still struggling to demonstrate a tangible financial return. The question, then, is perhaps no longer whether a bubble is forming, but rather how big it is and how violent its correction could be.

For Europe, this acceleration acts as a powerful revelation of its own weaknesses. The race for AI infrastructure consolidates the hegemony of American hyperscalers, who alone have the capital capacity to make such investments. As a result, the European economy's dependence on them, a recurring theme of concern in our previous notes, has deepened further. Initiatives in favour of a European "trusted cloud", although necessary, are struggling to scale up and now appear insignificant in the face of the striking power of American players. Europe finds itself in a position of structural dependence, forced to finance, through the purchase of services, the very infrastructure that underpins the dominance of its main competitor and unpredictable ally. The risk of entire sections of its economy being placed under supervision is no longer a mere hypothesis, but a political and industrial concern.

At the same time, the security threat has mutated, becoming more complex and dangerous. Generative artificial intelligence is not only a driver of productivity; it is also a powerful accelerator for cybercrime. We are witnessing the industrialisation of attacks of a new sophistication: automated and hyper-targeted disinformation campaigns, social engineering amplified by the use of virtually undetectable deepfakes, and the development of malicious code by AI capable of identifying and exploiting vulnerabilities at unprecedented speed. Organisations' exposure is growing exponentially, while the professionalisation of attackers, often backed by state-sponsored entities, is making defence increasingly costly and complex. The risk of digital chaos, which we have already mentioned, could be drawing inexorably closer.

Finally, this relentless race for computing power highlights the contradictions inherent in the concept of "digital sobriety". The explosion in energy consumption by data centres is in direct conflict with the goals of decarbonising the economy. The issue is no longer simply one of individual usage, but rather that of a model of technological development that seems to ignore planetary limits. This impasse calls for a profound reflection on a new form of digital governance. While trade-offs will have to be made in a context of tensions over electricity production, the question of the social utility of certain digital services, such as the most energy-intensive metaverses and AI, will become increasingly acute. In the absence of regulation and political vision at the European level, the imperative of sobriety risks being sacrificed on the altar of technological competition, in which Europe is, for the time being, merely a spectator and a customer.

However, it would be strategically dangerous to view artificial intelligence solely in terms of its risks and excesses. Despite these legitimate concerns, which are increasingly prominent in economic and geopolitical debates, practitioners now know without a shadow of a doubt that AI is an unprecedentedly powerful lever for organisational transformation. When deployed in a controlled and trusted environment, it is already proving to be a major tool for competitiveness and performance. In many areas, its applications can substantially enhance organisations' ability to create value, whether through spectacular productivity gains, an unprecedented acceleration of innovation cycles, or an increase in human creativity. By freeing its users from tedious or repetitive tasks, artificial intelligence does not replace humans. It liberates them by allowing them to focus on activities with the highest added value, where their judgement, intuition, creativity and strategic vision will remain irreplaceable for a long time to come.

In this exciting context, where the AI agent market is undoubtedly set to experience exponential growth, the pressure to act is strong and omnipresent. However, giving in to a blind race for power, limiting oneself to consuming the services of the largest and most generalist models, is increasingly seen as a strategic error. The real challenge for businesses is not only to adopt AI, but also to master it. This requires developing a unique strategic approach, capable of questioning the dominant paradigm in order to build solutions that are truly tailored to needs, effective and sustainable. The future undoubtedly belongs not only to large monolithic models (LLMs), but also to heterogeneous and agile architectures, in which smaller, specialised models (SLMs) can perform the majority of agentic tasks with far greater efficiency and simplicity. Seizing this opportunity means rejecting the inevitability of dependence in order to build real mastery, making AI a lever for competitive differentiation in the service of chosen and sustainable growth. The challenge for Europe is therefore not to suffer this revolution, but to embrace it in all its dimensions and invest heavily in making it an instrument of growth and progress in the service of its autonomy, competitiveness and the promotion of its values.

In conclusion, what kind of digital resilience does Europe need?

The picture painted in this note is that of a world in which traditional reference points are rapidly disappearing. They are giving way to a brutal international order, where competition for power, particularly technological power, has become the main grammar of relations between states. Faced with this upheaval, fatalism would be the worst possible response. On the contrary, it is in such a context of disruption that the imperative of digital resilience takes on its full strategic dimension, not as an additional cost or constraint, but as an essential condition for the freedom of action of organisations and the future prosperity of our continent's economy.

However, this resilience should no longer be viewed solely from the perspective of technical robustness or defensive posture. It must be considered an essential lever for competitiveness and a major competitive advantage. In an unstable world, the ability to anticipate disruptions, absorb digital shocks and adapt to them is not just a matter of insurance. It is now a differentiating factor that inspires market confidence and strengthens strategic positions. Digital practitioners are seizing on this requirement and transforming it into a weapon of positive conquest, serving the business and performance of their organisations. It is by building this digital resilience, not as a bulwark against the world, but as a platform for projection into it, that European companies will be able to unleash their full growth potential and that Europe, in turn, will give itself the means to exert influence in the new world order. It is to this ambition, both political and industrial, that this strategic policy report humbly intends to contribute.

Before allowing readers to engage with the forward-looking analyses introduced in this background note, I would like to extend my warmest thanks to the teams at Cigref and Futuribles who contributed to the preparation of this report. Their intellectual rigour, commitment and perseverance have been particularly valuable in navigating the complexities of our times. May this collective work provide everyone with the keys to understanding necessary to forge their own convictions and strategic decisions.

Henri d'Agrain, Director of Cigref

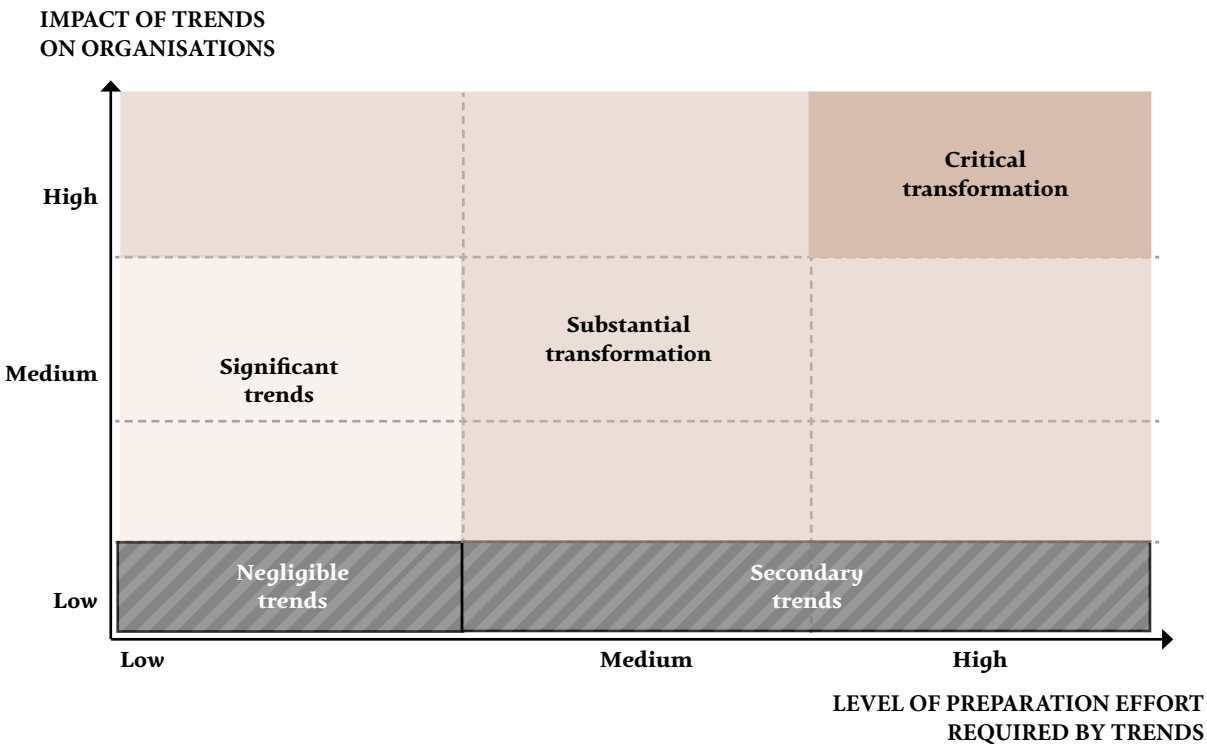
Objectives, ambitions and methodology of the report

The Strategic Orientation Report (ROS) aims to help Cigref members understand and prepare for the future. The objective is to support them in their strategic ambitions by providing them with rigorous forward-looking analyses of the main present and future transformations of the digital ecosystem. This mission involves disseminating a global vision of digital issues, placed in their context.
The forward-looking approach adopted allows us to take a step back from the changes currently underway in order to identify those that could have a truly transformative impact in the future and those that could open up new possibilities. **The *2025* edition of the ROS is a continuation of previous editions**, while also offering additional forward-looking analyses for the period up to 2040.

The first part of the report presents a forward-looking analysis structured around the five major areas of digital transformation identified by Cigref in its first ROS, namely: geopolitics, economics, technology, the environment and society. Without claiming to be exhaustive, this selection aims to offer the most cross-cutting approach possible to a subject as vast, diverse and changing as digital technology. For each of these areas, the main transformations at work have been identified, according to the following structure:

- **Major trends**, corresponding to trends with a strong impact and high inertia, and therefore likely to continue until 2040; these include several weak signals, i.e. trends that are currently minor in terms of scale and impact, but likely to develop over the next 15 years.
- **Disruptive hypotheses**, which may be more or less probable but, if they materialise, will have a major impact on digital organisations.

The second part of the report examines possible developments in the digital function itself, in order to anticipate the opportunities that each organisation could derive from the transformations described above. This forward-looking work consisted of identifying four archetypes capable of representing the digital function in 2040. Beyond the question "What might happen?", we considered possible developments in the digital function itself in order to adapt it to these transformations and define "what we could become".
The archetypes proposed are not, of course, models, and do not represent any particular organisation. They are primarily a basis for reflection, which digital departments can use to inform their strategic thinking. This will involve weighing up the opportunities and threats resulting from changes in the context against the strengths and weaknesses specific to each digital function. On this basis, the relevance of each archetype can be questioned in order to identify strategic priorities and the associated levers for action.



A summary diagram, included at the end of each ROS field, presents the main heavy tasks in the form of a matrix, ranked according to their impact on organisations using digital services and the preparation effort they require.

The last part of the report proposes principles for action to support Cigref members and players in the digital ecosystem in building resilient digital strategies for 2040. The cross-cutting elements presented are consistent with the analyses, according to the five major areas of digital transformation identified.

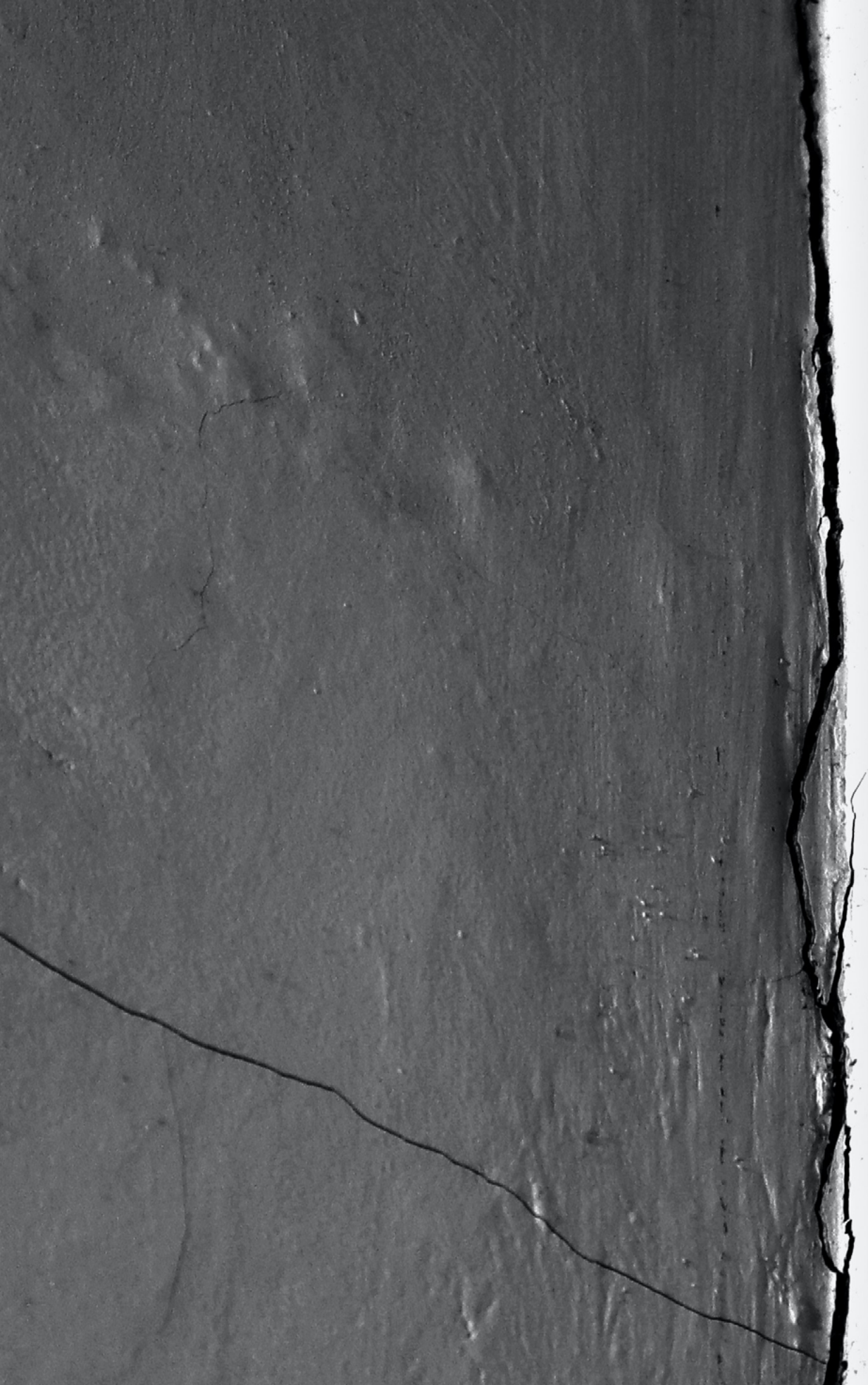
In terms of methodology and comitology, this report is based on:

- The work of the five previous ROS;
- The ongoing work carried out by Cigref's permanent team on these topics;
- The forward-looking monitoring work carried out by the Cigref project group and the Futuribles forward-looking consulting firm, based on a rigorous methodological approach;
- The contributions proposed by two Cigref bodies consulted during four workshops organised between January and June 2025;
  - **The Strategic Orientation Council (COS)**: composed of five Cigref administrators and five qualified individuals, this council defines Cigref's strategic orientation objectives each year, guides its work and provides expertise to ensure its quality.
  - **The Youth Strategic Steering Committee (COS Jeunes)**: created in 2022, this committee is composed of 75 employees under the age of 30 from 40 Cigref member organisations. It guides the work of this initiative in addition to the positions of the COS.

Part 1

Prospective analysis

This first part presents a study of the five major areas of digital transformation by 2040.



01 Field

Digital Geopolitics

Major trends and disruptive hypotheses

Major trends

Trend 1. The United States still maintains its technological supremacy, despite China's growing power

The direct and indirect rivalry between China and the United States continues to redefine the global balance of power and is increasingly exacerbated by the leverage of technological power. For several years now, this conflict has partly centred on one of the most critical stages in the digital value chain: semiconductors, which are key components in the defence, automotive, aviation, energy, telecommunications and finance industries, as well as in healthcare. If the United States retains its status as a superpower, it is largely due to its mastery of technologies associated with the semiconductor industry – from design to end use, including application integration and international deployment in terms of standards. This is where, according to many analysts, the global strategic pivot is at stake (*The Semiconductor War, the Global Strategic Game*, Chris Miller, 2024). At the same time, China is investing heavily to catch up with the United States, now spending more on chip imports than on oil and gas (IRIS).

The year 2025 is a key date for taking stock of the actions taken by these two players in terms of geostrategy, industrial policy and digital science and technology.

On the American side, Washington responded nearly 10 years ago to China's challenge to its hegemony with the tariff nationalism of the Trump I administration (50% tariffs on Chinese solar panels and household appliances), followed by the Biden administration with its industrial offensive (investigations, restrictions and an expanded blacklist: Huawei, CNOOC, China Mobile, etc.) pursued the same goal of slowing down China's move upmarket. The adoption of the CHIPS and Science Act marks a decisive turning point (McKinsey): $52.7 billion injected, $39 BILLION dedicated to domestic chip production, accompanied by a territorial exclusion clause targeting China and a massive tax credit (25%). In June 2025, this strategy evolved into an explicit industrial anchoring doctrine, with the lifting of distribution restrictions to secure allied demand and the announcement of colossal commitments with major players in the sector such as TSMC (c. $100 billion, Reuters), GlobalFoundries ($16 billion, Reuters) and Micron ($200 billion, Reuters).

On the Chinese side, Beijing's response is considerable and fits well with a logic of symmetrical confrontation, if not *"war economy through organised overproduction"* (*Bienvenue en économie de guerre*, David Baverez, 2024). Through tariffs on US$110 billion worth of exports, targeted restrictions on foreign direct investment and a refocusing on sovereign assets, **the doctrine of independence (if not technological self-sufficiency) of the "Made in China 2025" plan appears to be a common thread running through China's geopolitical action**. An industrial effort on a scale unmatched since the Maoist revolution has also been undertaken. In total, nearly $150 billion has been injected into China's upstream microchip supply chains, with the stated goal of reducing their technological dependence from 85% to 30% in ten years (Economist Intelligence Unit).

To date, however, China's acceleration remains constrained by US bans, resulting in a relative delay in the development and deployment of certain critical technologies ("Extreme Ultraviolet Lithography" for engraving latest-generation chips, "Electronic Design Automation" architectures for integrated circuit design, differentiating patents). Despite partial short-term success, the Trump administration's restrictions on exports of H20 chips to China – intended to preserve the US lead – have nevertheless had the side effect of accelerating China's efforts to circumvent, build resilience and innovate under pressure (Economist Intelligence Unit). This situation has led to a drastic acceleration in the decoupling between China and the United States, with each country threatening the other with a trade embargo, forcing American and Chinese policymakers to accelerate their transition to autonomy in parallel.

By 2040,

this trend could signal a return to spheres of influence and quasi-exclusive blocs. The techno-industrial duel is therefore likely to play out on an increasingly broad stage, that of indirect normative and strategic confrontation. Indeed, the failure of the "Nixon II" strategy, with which the Trump administration hoped to detach China from Russia, has led to a strengthened alignment of the BRICS countries, and of these two countries in particular, around Taiwan (The Great Continent). In order to avoid facing several major fronts at the same time, the United States seems forced to focus primarily on competition with China, either directly in the Pacific or indirectly in the Middle East. This is to the detriment of its security support position in Europe, particularly in Ukraine. In these circumstances, Beijing could then use Taiwan to project its digital power, while Moscow could increase its leverage for destabilisation.

A new bipolar pattern could therefore emerge, with a technological front line that does not reflect the dynamics on either side: China advancing through the systematic integration of AI, the United States locking down the race for disruptive innovation and hardening its position, and the countries of the European Union remaining caught between the two blocs without any power of their own, seeking a third way through cooperation. The dynamics of US hegemony could continue to erode slowly, despite the maintenance of its technological superiority. Competition between states would then focus less on volume and more on critical layers of control and the ability to convert industrial power into "cognitive sovereignty". China could be tempted to accelerate at an unprecedented pace in the run-up to the centenary of the Maoist revolution, in 2049.

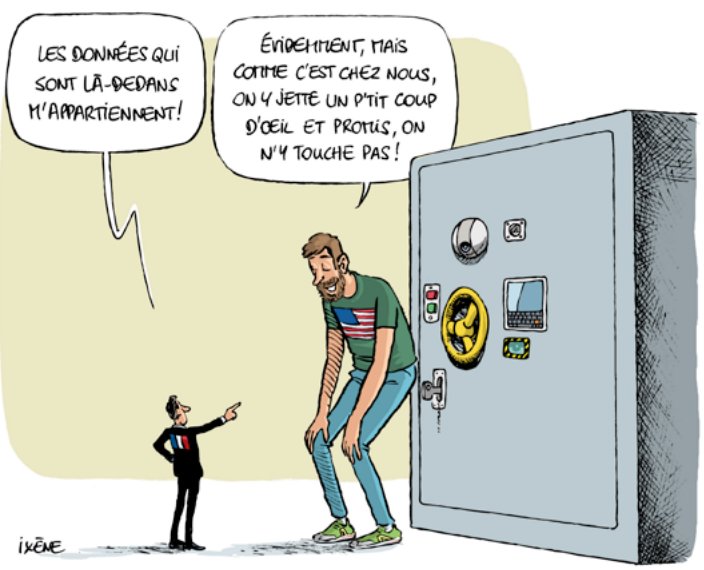
Trend 1.

Trend 2. Relations between the United States and the European Union are clouded by uncertainty regarding business continuity and data transfer

Since Donald Trump's second inauguration on 20 January 2025, scenarios involving a disruption in the supply of American digital services to Europe no longer seem to belong solely to the realm of "political fiction". Against this backdrop of geopolitical volatility, numerous initiatives have been launched to reassure European organisations at the highest decision-making level. Nevertheless, these organisations are still affected by the same upheavals that are shaking the international institutions inherited from the post-Second World War era and the geopolitical order that has been in place since the end of the Cold War.

The commitments made in Brussels at the end of April 2025 by Microsoft President Brad Smith are enough to highlight, on the one hand, the unease and growing suspicion that have taken hold in transatlantic digital relations and, on the other hand, the commercial potential that the still ill-defined market of "European digital sovereignty" (Microsoft) represents for the coming decade. For example, the desire to add a legal counterattack clause to new Microsoft contracts in the event of attempted interference by the US administration undoubtedly fuels an illusory sense of Europe's resilience, despite its current state of advanced digital dependence on several critical technological layers. Worse still, the impression of uncertainty and increasing exposure to the scope of Executive Orders has been considerably reinforced following the disconnection of Microsoft services from the Chief Prosecutor of the International Criminal Court (ICC), in connection with the sanctions adopted by Trump against the ICC, following the arrest warrants issued by the ICC against Israeli Prime Minister Benjamin Netanyahu (DataNews).

The political direction taken by the new Trump administration supports this trend of locking in American positions through law and standards and constitutes the legal counterpart to economic warfare, known as lawfare. This is evidenced by the deliberate fragmentation, in the early days of President Trump's second term, of the Privacy and Civil Liberties Oversight Board (PCLOB), which oversees compliance with American surveillance laws. This US body was previously responsible, among other activities, for ensuring compliance with transatlantic data transfer agreements, known as the Transatlantic Data Privacy Framework (TADPF). The PCLOB's independent oversight mechanism was a pillar of the agreement adopted with great fanfare in July 2023 under President Biden, replacing the Privacy Shield, which had already been invalidated (Schrems II, 2020) by the Court of Justice of the European Union (CJEU), following the invalidation ten years ago of the Safe Harbor (Schrems I, 2015). The protection guarantee offered by the PCLOB is not based on laws passed by the US Congress but on presidential orders and fragile diplomatic commitments, which can be revoked at any time by a simple decree that does not have to be made public (Euractiv).



By 2040,

the absence of safeguards could call into question all data transfers between the United States and the European Union and, by extension, the GDPR and all the regulatory mechanisms developed over the last decade. The situation already exposes hundreds of thousands of European companies and administrations to unprecedented legal uncertainty. It could also jeopardise the continuity of European digital services relying on US infrastructure. As such, the vast majority of cloud and artificial intelligence services could be at stake, given the dominance of American hyperscalers in this digital segment.

Trend 2.

Trend 3. Countries in the "global North" are gradually handing over responsibility for their sovereign digital services, critical infrastructure and essential data

For several years now, the operational, investment and research capabilities of digital giants have quantitatively exceeded those of public authorities in many strategic areas. Countries in the "Global North" are transferring technological control of segments falling within their sovereign prerogatives to transnational companies.

The United States undoubtedly best illustrates this ongoing evolution, to the point that some analysts are talking about the birth of a new military-industrial complex or integrated "techno-nationalist" ecosystem (Le Grand Continent). On the one hand, the relationship between national innovation and political success is being questioned by the joint investments of Marc Andreessen (Shield AI, Alduril, Skydio), Palmer Luckey (Alduril) and Eric Schmidt (Rebellion Defence), which have exceeded £100 billion in start-ups specialising in defence technologies over the last four years. On the other hand, it is the intertwining of nation and technology that is targeted by the meteoric rise of a company like Palantir, co-founded by the highly messianic Peter Thiel, one of the radical figures of Silicon Valley's techno-libertarian movement, also known as the "Dark Enlightenment " (Le Grand Continent). This start-up has quickly become a central player in the US government's infrastructure, to the point where it now publicly states its goal of becoming the "operating system of the US government" (FrenchWeb). The analysis and decision-making support activities delegated to this private company in key areas of public decision-making – intelligence, healthcare and hospitals, defence, tax agencies, logistics – reflect a hybridisation between the private sector and the state apparatus, going so far as to integrate it into the final link in the military chain of command, the "kill chain".

Several other American tech giants, with sufficient critical mass to absorb technological disruptions, are involved in programmes directly affecting US sovereignty: the Pentagon's critical cloud and military data management (Joint Warfighter Cloud Capability for Microsoft, affected by the scandal of military cloud systems being maintained in China, according to Clubic), tactical orbital internet (Starshield), tactical augmented reality (HoloLens for Anduril and Microsoft), AI defence against drone attacks (Anduril, OpenAI, Anthropic, Google and xAI), deployment of high-speed internet in rural areas (Space X and Microsoft Azure Space), nuclear reactors for data centres (Microsoft and Constellation Energy for the relaunch of the Three Mile Island power plant, Amazon and the development of X-Energy SMR reactors, Google and the order for a fleet of molten salt reactors from Kairos Power, Meta and Constellation Energy).

By 2040,

the ability of states to assess and act in many critical areas could become dependent on private companies' tools, whereas these tools were only intended to be levers for improvement. The weight and influence of private actors could, on the other hand, profoundly call into question the impartiality of internal arbitration – decision-making capacity – and the diplomatic strategies adopted by states at the international level, especially when the digital interests of these giants are at stake.

Trend 3.

Trend 4. Technological dependencies are increasingly perceived as sources of vulnerability, and strategies are being implemented to promote digital resilience

Dependency characterises a relationship between two or more parties. In many cases, technological dependency is not only a matter of quantitative, economic criteria, but also of qualitative factors, particularly geopolitical ones. It cannot therefore be measured solely in terms of market share or budget lines, but also has a strategic dimension. From the customer's perspective, digital dependency can quickly become a critical vulnerability when service continuity is compromised for reasons that are not solely economic.

The Russian-Ukrainian conflict revealed the deep energy dependence of part of Europe. The instability of the global context particularly highlights the consequences of technological dependencies that have been accepted for more than twenty years on a *de facto* **oligopoly** composed of only a few producers of digital products, services and platforms of the same nationality. In Denmark, technological dependencies on mainly American players have been considered by several public actors as a source of critical vulnerability for the independence and sustainability of public organisations. The country's two main cities, Copenhagen and Aarhus (Usine Digitale), have therefore launched a programme aimed at reducing the risk associated with their dependence on Microsoft software and cloud services, while the Kingdom's Minister for Digital Affairs, Caroline Stage, announced the phasing out of Microsoft solutions within her administration (Politiken). For similar reasons, the German state of Schleswig-Holstein announced in early June a major transition marked by the gradual abandonment of Microsoft software for its 60,000 employees in favour of open source solutions such as Linux, Open-Xchange, Nextcloud and Thunderbird (France 24). At the same time, the European Commission also began serious discussions about switching from Azure to OVH cloud (Le Monde Informatique). The discourse is therefore changing in nature and increasingly focusing on the scope and thresholds of geopolitical risk acceptability as a consequence of technological dependence.

> ***Approaches to controlling dependencies through risk management are not identical to digital sovereignty strategies: they belong to two distinct categories.***
> *On the one hand, the quest to reduce risks is mainly driven by realism within organisations: by 2040, the deciding factors for digital function should favour a substantial commitment to security and governability, taking into account geopolitical risk beyond any idealism or ideology. As part of these considerations, a case-by-case assessment should be made of the degree and manner of cooperation or alignment with the policies of the extra-territorial states in which the organisations operate.*
> *On the other hand, the quest for sovereignty depends on states and, a fortiori, on government. When the activities of certain organisations are considered essential (OIV or OSE, for example) and are de facto subordinate to the sovereign prerogatives of states, the autonomy strategies of these actors cannot ignore the sovereignty strategy of their state.*

By 2040,

the new geopolitical balances currently being managed should now be entering a phase of maturity. For user organisations' strategies to control the risks associated with technological dependencies, **success will depend on their ability to secure a choice not only among several economic players, but also among suppliers of different nationalities**. This capacity for action must also extend to contractual conditions that are essential from a geopolitical perspective: contractual reversibility and rescheduling, interoperability and control of data governance, availability of services **in the event of diplomatic breakdowns and internal upheavals.**

Trend 4.

Trend 5. Conflicts are shifting to the digital sphere and logical weapons are becoming a differentiating lever of power.

Alongside the physical theatres of high-intensity conflict between Russia and Ukraine, Israel and Iran, and India and Pakistan, the exponential growth in data flows continues to reinforce the importance of the digital realm as a battlefield. Strategies for preserving or expanding national interests are shifting massively towards the electromagnetic, electronic and cyberspace domains and, in order to ensure their long-term influence, are involving "the militarisation of thought itself, cogitation". According to David Colon, in his book *La Guerre de l'information* (*The Information War*), States in the conquest of minds, two distinct dynamics of digital influence illustrate the phenomena of information warfare and cognitive warfare: on the one hand, that of an intentional tactic of "jamming" perceptions by saturating them with contradictory news, as proposed by Donald Trump's former communications adviser, Steve Banon; on the other hand, a permanent war targeting the judgement capabilities of the intended target. In one case, the aim is to engineer chaos, divide natural communities, disengage people from information, stun and erode their discernment, and spread a feeling of exhaustion and powerlessness; in the other, it is competition, contestation and confrontation to bring about behavioural change through lasting and profound modification of civilisational structures.

The Western context of relative freedom of information circulation particularly exposes organisations and populations to this indirect warfare. The digital space in the broad sense has therefore become a necessary prerequisite for hybrid and epistemic geopolitical warfare, insofar as the "logical layer" of applications, software and code significantly shapes the "semantic layer" of social etiquette. Of course, disinformation and propaganda have always been part of communication strategies. The differentiating factor today is the considerable reduction in the costs of producing, sharing and consuming information (Psychological Defence Research Institute, Lund University). In this sense, the proliferation of information and storytelling platforms, the global interconnection offered by social networks, the massification of generative AI, and the ongoing democratisation of deepfake models and other non-kinetic weapons have accelerated the digital phenomena of "fog warfare" and "echo chambers", pushing them to the algorithmic level (Special Competitive Studies Project).

By 2040,

the increase in operational capabilities brought about by the digitisation of the battlefield should make "logical weapons" a differentiating factor in geopolitical power (*Hyperwar, How AI is revolutionising warfare*, Dr Jean-Michel Valantin). In light of the tsunami of Iranian cyberattacks in June 2025 simultaneously targeting critical Israeli infrastructure and actors – such as banks, media outlets, hospitals and government agencies – there is every reason to believe that by 2040, digital weapons could be considered a form of "power equaliser", an alternative to nuclear weapons. The competitive advantage of digital weapons lies in the human ability to integrate their systems into the chain of command without risking cognitive overload from an excess of information that is counterproductive to decision-making (Revue de Défense Nationale). However, their acquisition will depend on sovereign technological innovation and stable, long-term command capabilities, particularly from the private sector. This is one of the reasons why autonomy in defence equipment cannot be achieved without strategic autonomy in the digital domain, which is itself supported by a set of resilience strategies and "anti-fragile" mechanisms to deal with hybrid and asymmetric warfare.

Trend 5.

Trend 6. The intertwining of value chains and the increase in attack capabilities are accelerating international cooperation on cybersecurity and cyber defence

Cyberattacks are becoming increasingly sophisticated, incorporating artificial intelligence to automate and target campaigns. Exploiting vulnerabilities – upstream – in increasingly intertwined supply chains and – downstream – in connected objects and unpatched software flaws, cybercriminals are expanding their attack surface. The most worrying attacks now target trusted suppliers themselves, such as Microsoft, Fortinet and SolarWinds, exploiting edge equipment (VPNs, firewalls) and the human factor in unprecedented ways to bypass deep defences.

The growing overlap between state espionage, hacktivism and cybercrime is also one of the key developments of 2024 (Cyber Threat Landscape). Tools and infrastructure are sometimes shared between state actors and cybercriminals, blurring the lines – as in "false flag" attacks – and allowing capabilities developed for espionage programmes to be diverted for criminal or activist purposes (Ministry of the Interior). The rise in distributed denial-of-service attacks – DDoS attacks doubled in 2024 compared to 2023 – reflects the intensification of strategies to destabilise critical systems, while the increase in attacks targeting capabilities reinforces the threat of operational capacity degradation, particularly in industrial systems (SCADA). Similarly, attacks by state actors targeting hyperscaler infrastructure are intensifying. Furthermore, the expansion of capabilities offered by private offensive cyber warfare companies (such as the Israeli company NSO Group, which developed the Pegasus spyware) reflects the widespread use of software weapons beyond the state sphere (Cybernews).

Faced with these geopolitical challenges, the level of cybersecurity is set to be raised by a series of defensive laws. These include the SREN transposition law in France, European directives such as NIS2 for risk management in critical sectors, DORA for the standardisation of resilience policies in the financial sector, the CRA to strengthen the cybersecurity of digital hardware and software, the revision of the Cyber Blueprint for interactions between multiple stakeholders (European agencies, national CSIRTs, EU-CyCLONe, CERT-EU, etc.) and the upcoming revision of the CSA for the legal framework for cybersecurity certification schemes. Despite this legislative framework, international cooperation remains a vital condition for resilience. Major operations to dismantle malicious actors (Matrix, Breach Forums, clandestine telephony in prisons) have only been possible thanks to operational interoperability between ANSSI, Europol, Eurojust, Interpol and national services.

By 2040,

the various tactical shifts should have completely redefined digital trust: on the defensive side, the a priori mistrust of cyber "Zero Trust", the explicit nature of repeated trust, "authorisation-as-a-service" and "contextualisation of trust" should be part of everyday commercial relations as part of a global reshaping of geopolitical alliances. On the offensive side, collective trust and resilient cooperation in cybersecurity should become essential levers for overcoming the fragmentation of international relations and ensuring the continuity and effectiveness of large-scale solutions.

Trend 6.

Trend 7. The temptations of a splinternet are growing

The "splinternet" (or fragmented internet), already in the making, represents a weakening of the deterrent power that had previously been provided by the interdependence of global networks. It marks the transition from a universal internet to a digital grammar of the world in blocks, where connectivity remains, but where unity and alignment around common spaces are fading in favour of new power relations. The architecture of the internet, long thought of as a neutral, global and interoperable space, is becoming a reflection of divergent and irreconcilable world views. **Technical, regulatory, commercial and geopolitical changes are simultaneously making it increasingly possible – and for some actors increasingly desirable – to gradually shift towards a fragmented internet, with fragmented, territorialised and potentially conflictual governance** (IFRI). This retreat is reinforced by the growing marginalisation of international technical coordination bodies (ICANN, IANA, UN, WIPO), whose legitimacy in establishing a universal framework based on de facto regionalised infrastructures (multiple DNS root servers, five Regional Internet Registries for IP address management) is increasingly being challenged. Nevertheless, regulators can still become architects of regional resilience within limited and controlled areas of interoperability and openness, despite the archipelagoisation of digital technology.

> ***Four blocs with clear techno-political contours are already emerging beyond Europe.***
> ***In the United States**, the instrumentalisation of the privatised backbone of the internet represents one of the key determinants of its 'fragmentation': globalisation functions as an instrument of extraterritorial power, subject to less formal regulation and counterbalanced by a strong capacity for coercive normative projection (export sanctions, Cloud Act).*
> ***China** is pursuing a policy of civilisational regulation through its "Great Firewall", which is not only an information barrier, but also acts as a lever of control, a vector for innovation and an instrument of projection, as evidenced by the e-yuan project, a digital central bank currency (MNBC).*
> ***Prime Minister Modi's India**, caught between these two blocs and despite its ambivalent position, aspires to "self-sufficiency" and is multiplying sovereign digital initiatives beyond its status as a "superpower of IT outsourcing" (ORF).*
> *Since 2019, **Russia**, with RuNet, has been experimenting with voluntary strategic isolation to acquire digital independence, based on a Russian twin of the global internet capable of withstanding any form of disruption.*

In this fragmented landscape, Europe seems to be taking on the role of regulator. The GDPR, the SREN law, the NIS2 directive and the Data Act are evidence of an effort to anchor digital sovereignty in cooperative action. However, this approach risks being undermined by technical realities if it is not backed by an autonomous infrastructure (sovereign cloud, IXPs, localised DNS resolvers) and coupled with a collective industrial project worthy of a potential "digital industrial and technological base". Amazon Web Services' "Sovereign EU" cloud already seems to illustrate this tension: sovereignty promised through internal decoupling of the European platform rather than through external control.

By 2040,

the proliferation of targeted Internet shutdowns could have led to a segmentation of the global network based on deliberate political alignment strategies, going well beyond simple technical friction. The universal Internet could have given way to normative archipelagos where the establishment of businesses (Department of State), data circulation, connectivity architectures and even access to the Internet would be conditioned by the digital sovereignty of each state, according to their membership of different geopolitical blocs and their role in each sphere of influence. The internet could therefore become a critical resource in its own right, on a par with raw materials or energy. Local technologies – territorialised 5G, edge computing, data centres – could then structure restricted trade corridors. Furthermore, IP re-addressing mechanisms (France 24), coercive rerouting and invisible compartmentalisation through political filtering could result in a new kind of digital border mapping (Hérodote). In this context, the "Splinternet" may no longer be a regrettable trend in European countries, but rather an accepted framework that allows regional resilience to take precedence over global interoperability through the successful Recursive InterNetwork Architecture (RINA) project (La revue européenne des médias et du numérique).

Trend 7.

Hypotheses of disruption by 2040

1. In a context of high tension, the United States cuts off access to its digital services to one or more competing countries.
The geopolitical advantage gained from technological advances could represent a diplomatic lever and a differentiating factor in terms of power. The widespread practice of restricting exports of IT equipment and deliberately cutting off Internet access could increase the temptation to abruptly and repeatedly cut off access to all digital services. Hegemonic countries in the digital sphere, such as the United States, could cancel the provision of certain digital services in the event of geopolitical disagreement.

2. Private actors are becoming political and geopolitical players on a par with states and are developing their own diplomatic alignment strategies.
The rise of technology companies in many critical areas could give these private actors capabilities for action, influence and resource management comparable to those of states. In a fragmenting world, their strategies of alliances and misalignments with the policies of the states where they operate could have direct consequences on regional and global geopolitical balances.

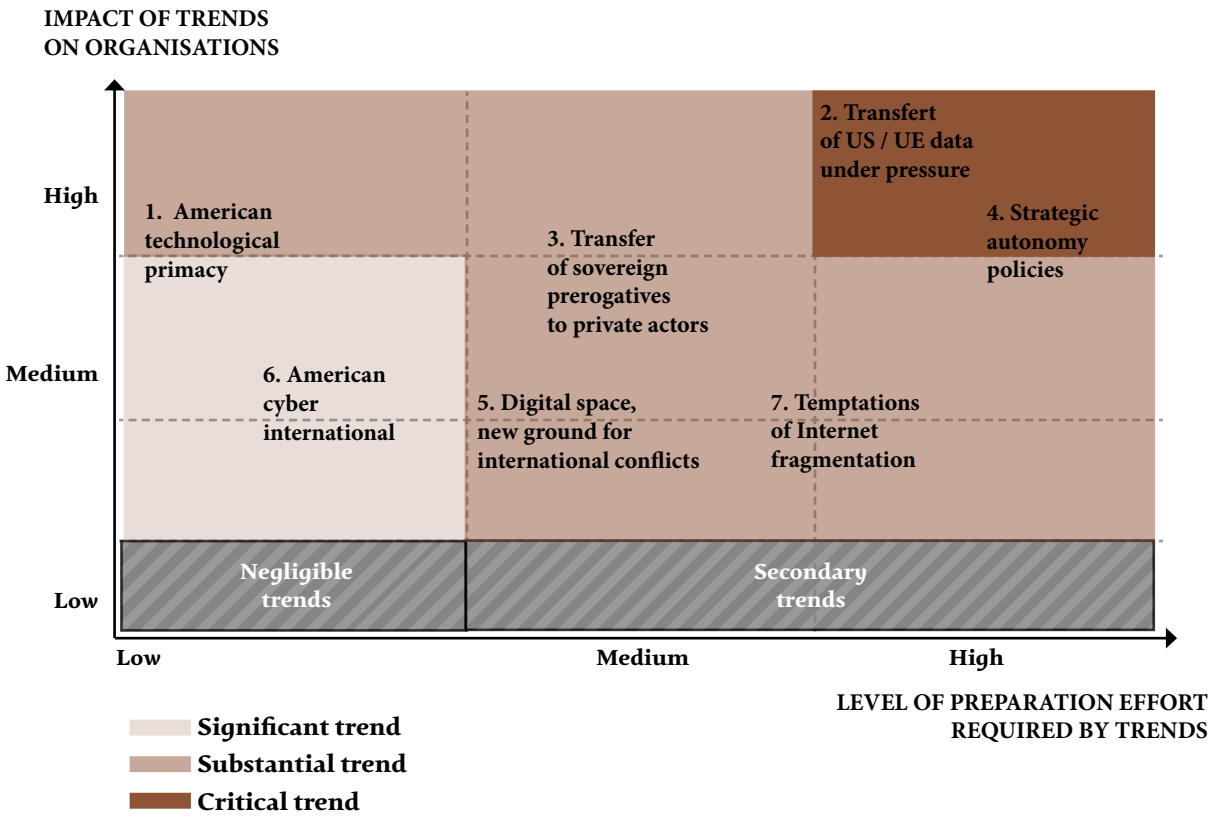
3. The EU is making it mandatory to diversify suppliers of digital products and services.
The scope of European players' technological dependence on third parties continues to grow, while demand for digital services is skyrocketing. Taking into account the geopolitical consequences of these dependencies, the European Union is imposing a maximum threshold of 50% market share concentration in the hands of players of the same non-European nationality. The forced redefinition of value chains could give rise to new intra-European alliances and enable the unification of the European digital market.

4. Between 2030 and 2040, a high-intensity solar storm hits the Earth, depriving organisations of their electricity and communication networks for months.
The vulnerability of digital and electrical infrastructure to major cosmic events remains underestimated. A solar flare of exceptional intensity could potentially strike the Earth, saturating the magnetosphere and causing prolonged failure of electrical networks, satellites and communication systems. Preparedness for situations of degraded services and activities, and strategies combining high-tech and low-tech solutions, would then be competitive advantages.

5. A substantial part of the internet is privatised.
The fragmentation of the global network and the rise of proprietary infrastructure could lead to the privatisation of entire sections of the Internet. By 2040, interconnection protocols, routing services and content distribution architectures could be largely controlled by private consortia, redefining the conditions of access, circulation and governance of data. In response, Europe could finalise an alternative public project to the historic TCP/IP protocols, establishing a resilient, interoperable and sovereign European Internet based on Recursive InterNetwork Architecture (RINA).

Summary
Field 01 – Digital Geopolitics

Major trends effort matrix



Reminder of the assumptions for disruptions by 2040

1. In a context of high tension, the United States cuts off access to its digital services to one or more competing countries.
2. Private actors become political and geopolitical players on a par with states and develop their own diplomatic alignment strategies.
3. The EU makes it mandatory to diversify suppliers of digital products and services.
4. Between 2030 and 2040, a high-intensity solar storm hits the Earth, depriving organisations of their electrical and communication networks for months.
5. A substantial part of the internet is privatised.

02 Field

Digital Economy

Major trends and disruptive hypotheses

Major trends

Trend 1. The "datafication of the world" is exponential, and fewer and fewer areas are spared.

The increase in market power enjoyed by Big Tech companies is reflected in a spectacular and record acceleration in their financial revenues. The club of companies listed at over $1 trillion on the Nasdaq continues to grow, leading the New York Stock Exchange to no longer refer to GAFAM or the "Magnificent Seven", but to BATMAAN to describe the American digital giants Broadcom, Apple, Tesla, Microsoft, Meta, Amazon and Nvidia (Le Figaro). The combined business volume of these companies reached more than $2 trillion for the year 2024, with net revenues of nearly $500 billion and a market capitalisation of just over $16 trillion in the second half of 2025.

Admittedly, the results of these few players are not entirely consistent if we compare the relative erosion[1] in the market share of Microsoft operating systems, or the sharp decline in Tesla's commercial, technological and reputational standing, with the commercial and financial explosion of Broadcom, a key player in semiconductors and software solutions, or that of Nvidia, which specialises in key microprocessors for AI. However, the emerging trend clearly shows that, for users of digital products and services, there is a continuous expansion of technological dependencies on the multiple services offered by this handful of players, with a cumulative increase over five years of 80% in their turnover[2] and 150% in their net profits.

In terms of business models, the apparent free nature of traditional digital services (search engines, social networks, mapping) **has served as a "Trojan horse" for the establishment of a behavioural extraction economy**. Personal data (searches, reactions, preferences, geolocation) has been converted into commercial profiles, then into advertising targeting spaces[3]. Some uses go even further in their capture, to the point where the press[4] is gradually being absorbed by platform and AI logic. Some journalistic content feeds, sometimes without compensation, into simplified formats designed to maximise advertising engagement. The signing in 2021 of the contract between the Alliance de la presse d'intérêt général (APIG) and Facebook, intended to regulate these uses, only really took effect two years later, with the creation of an operational collecting body, the Société des Droits Voisins de la Presse (DVP). This time lag illustrates a structural asymmetry: while national courts operate on a long time scale, GAFAM companies mobilise regulatory, algorithmic and commercial agility, which only belatedly and retrospectively slows down their data collection. Intellectual property therefore seems caught between economic expansion and democratic slowness.

New practices are beginning to transform the business models of these giants. In addition to introducing premium services on apps (Amazon, Apple, and Google), AI models are now attempting to limit the cost of their training data by drawing on user posts on the platforms to which they have access. This is particularly the case for adults who have not explicitly expressed their opposition on Meta (Data Protection Authority) but also on X, where the data feeds into the Grok model (ZDnet). Although enhanced filtering measures have been put in place by both companies to ensure that personal data is not stored during the training of AI models, the massive and default use of these social interactions raises questions about the limits of the European GDPR's scope of protection. This is particularly true in an era of systematic integration of artificial intelligence into the functionalities of these platforms (Gemini Livre, Traduction, Chromie, Flow, Deep Research, Imagen 4, Veo 3, Agent Mode, etc.). Under these conditions, social space and all common goods become a raw material with marginal cost, available by default. Their industrial exploitation leads to a strengthening of the platform effect (Metcalfe's law) and a major normative asymmetry between regulators and operators, leaving fewer and fewer spaces untouched by this datafication of the world.

1- In January 2009, approximately 95% of all desktop computers worldwide ran on the Windows operating system, a figure that is "more than" 72% in 2025.
2 - $2,072 billion in 2024 vs. $1,145 billion in 2020 for revenue and $489 billion vs. $199 billion. This calculation was made using data available on the reference website rendementbourse.com
3- Prompting intervention by the CJEU against social media platforms and networks, which invoke "a legitimate interest in targeting users with advertising"
4- The press is supposed to guarantee "humane, tangible and original treatment of current events" according to the three criteria that constitute copyright French

It is interesting to note that this logic of "generalised data capture" is reflected in the new practices of cybercriminals. Ransomware attacks are increasingly being abandoned in favour of data theft and resale, through the sale of infostealers, phishing campaigns and scraping scripts. This approach, which has become so industrialised that it can be described as Cybercrime-as-a-Service, is more discreet, less technically complex and less criminally engaging. It allows for broader and faster monetisation of information, which is generally stolen at low cost but in large quantities, from several different clients (Ministry of the Interior).

By 2040,

the expansion of a new business model based on direct capture within the ecosystem specific to digital giants should accelerate the process of datafication of the world and its economic exploitation. Data management by intelligent agents – agentic AI – should also lead to a profound restructuring of the digital economy, the labour market and skills: information would no longer be sought and explored, but delivered, recomposed and guided, to the point of disrupting the current economic structure of the web (search engines, SEO, centralised referencing and advertising) in favour of Generative Language Optimisation (GEO). The shift from B2C (business-to-consumer) to B2A (business-to-agent, or B2A2C) commercial segmentation could reflect this reconfiguration: users would then have to interact with autonomous agents, which would become interfaces, filters, transactional engines and even actors working on their behalf or in their place. Questions regarding design and digital communication, training adjustments and recruitment associated with such technological disruptions remain open, with the possibility of a proliferation of ultra-technological spin-offs from traditional companies seeking to avoid the costs of upskilling or reskilling their staff, at the cost of the certain demise of the original entities and a brutalisation of the social fabric.

Trend 1.

Trend 2. The economic consequences of technological dependencies are widening the competitiveness gap between Europe and the United States

The French digital economy is divided into three main segments: cloud and software (approximately 40%), digital services companies (approximately 50%), and technology consulting (approximately 10%). This ecosystem represents nearly €70 billion in activity for 2024 (Numeum), an increase of nearly 50% over 10 years (Institut Mines-Télécom). However, cloud migration and developments in generative AI are driving market transformation and productivity, with annual growth of more than 8% for the cloud and software segment alone, which represents 40% of the overall French market and is operated mainly by non-European players.

This repositioning in the value chain has a direct impact on the activity of digital services companies. In an environment where cloud solutions are perceived as immediately operational, scalable and driven by integrated innovation, the traditional intervention model of digital services companies seems to be becoming less central. In a move towards disintermediation, companies seem to be increasingly favouring packaged offers, managed services or high value-added platforms, to the detriment of more fragmented and time-consuming services. **In this context, the decline in digital services companies' activity (-2.1% forecast for 2025, according to Numeum) may not only be due to a slowdown in demand, but also to a long-term strategic shift that will shape organisations' technological investment choices.**

> *At European level, digital expenditure will represent, by 2025, an average of 2.2% of the turnover of large organisations using cloud and software and 45% of their current IT budget (Cigref x Asterès). Admittedly, there is considerable diversity in the resources allocated to this segment, mainly because the integration of digital technology into the core businesses of large organisations[1] varies greatly between sectors. However, in terms of cloud and software, the vast majority of players are affected by both the current growth in demand, estimated at 15%, and the current growth in prices, estimated at 10%.*
>
> ***Given the scissor effect of rising prices and demand, serious questions arise about the viability of the business models of organisations using cloud and software services.*** *The continued inflation of prices is linked to the hegemonic position of a handful of players, notably the three hyperscalers AWS, Azure Cloud and Google Cloud, which together account for 80% of the European market share. In addition, nearly 80% of the value created in this segment comes from the United States and Western Europe.*
>
> ***In France, orders from organisations destined for the United States in the cloud and software segment alone amount to €4 billion****, which is practically equivalent to the total budget for non-salary[2] defence expenditure (€47 billion for 2024).* ***For Europe, this share of the digital bill amounts to €264 billion****, which is comparable to its energy bill.*

Although they represent a hindrance to European competitiveness, the economic consequences of technological dependencies are not reflected in official data and figures. This is not only because the global statistical framework inherited from the post-war period does not give any tangible existence to digital service flows, but also because there is a total lack of transparency surrounding these service flows, which systematically pass through Ireland for tax reasons, a practice known as the "Double Irish". The "by-design" financial optimisation practices for digital flows are consciously and conscientiously organised to take advantage of average effective tax rates that are two to three times lower (Polytechnique Insights).

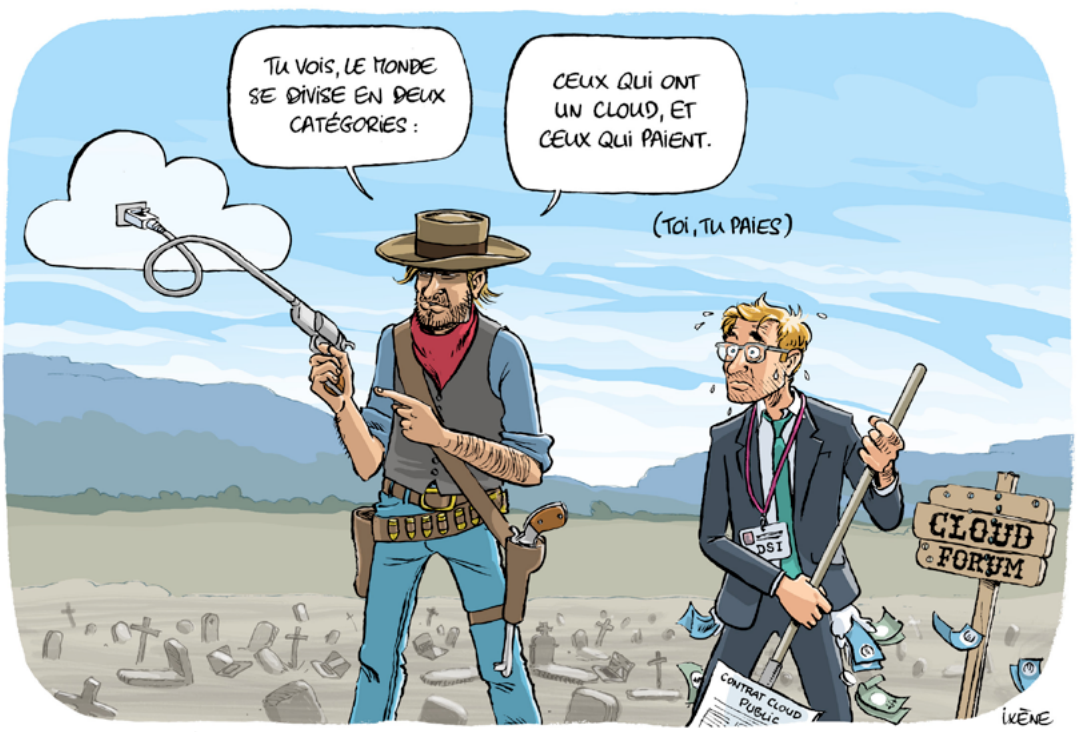
This lack of knowledge about actual flows comes at a time of growing economic tension in the coming years. The recent questioning of five years of efforts to achieve minimal global tax harmonisation is a sign of this. The G7 recently agreed – in exchange for the withdrawal of Article 899 from the Trump administration's tax bill, also known as the "revenge tax" – to exempt US companies from the two tax mechanisms proposed by the OECD[3], which set a minimum effective tax rate of 15% for organisations with a turnover of more than €750 million (Les Echos).

1- For example, the IT budget for the banking sector represents approximately 15% of the equivalent in turnover of the GNP and less than 5% for the agri-food sector.
2- The balance is part of the remuneration allocated to military personnel according to their rank, grade, qualifications and titles, or the position to which they are appointed. Benefits in kind may also be added to this.
3- The core of the OECD's proposed system, known as "Pillar 2", provides for a minimum effective tax rate of 15%, applied on a country-by-country basis. Pillar 2 includes a first rule (IIR), which places the tax adjustment burden on the parent company's country, and a second rule (UTPR), which allows other countries to tax uncovered profits. The United States remains an official member of the OECD's "inclusive framework" and continues to participate in discussions on Pillar 1, concerning the taxation of digital giants.

By 2040,

two opposing trends could be observed: on the one hand, a deliberate reorientation of digital flows, favouring European players; on the other hand, a widening of competitiveness gaps due to price increases by private players or US export taxes (Les Echos). In one case, the reallocation to the European market of just 15% of cloud and software purchases, through public procurement and joint private investment, could represent an economic footprint of €75 billion in turnover, nearly 500,000 jobs for businesses, €16 billion in public revenue and an improvement in the EU's current account balance of €100 billion over more than ten years[1]. In the other scenario, without the rapid and long-term exercise of some form of countervailing power, the annual amount of cloud-software services imported from the United States by European organisations could reach €900 to €1 trillion[2], an increase of 300% in 15 years.

Trend 2.



1- Assuming an average price increase of 10% per year for cloud and software services, redirecting 15% of previously targeted purchases would represent a reduction in imports of €100 billion over ten years.
2- Preparatory work for the Asterès study has enabled an initial estimate of €685 billion in European expenditure by 2035 to be drawn up, taking into account the rate of increase in both price and demand trends. By 2040, this figure could rise to nearly €900 billion, and to over €1 trillion if an export tax of around 15% were added.

Trend 3. The scope of digital dependencies is expanding with the absorption of strategic infrastructure by digital giants

The latest "digital revolution", based on cloud technologies, artificial intelligence and, ultimately, quantum acceleration, relies fundamentally on computing, storage and network capacity, i.e. on hardware computing infrastructure, telecommunications infrastructure and carbon-free energy production infrastructure. **Information itself is certainly contested, but so too are the technical equipment that produces, stores and transports it**. The silent capture of strategic infrastructure by hegemonic digital players, coupled with market forces, is contributing to the expansion of digital dependencies.

Numerous strategies appear to have been put in place to perpetuate the positions acquired through technical lock-in, economic incentives and information asymmetry regarding business models. As digital technology becomes the universal medium for industrial, administrative and social activities, dependence on cloud services and software infrastructure no longer seems to be a rational choice for optimisation, but rather an unconsidered necessity imposed by market forces.

The initial interdependence, beneficial in terms of commercial openness or alliances, becomes a unilateral constraint when a player locks in a critical stage of the value chain, with no substitutable, equivalent-level recourse to ensure essential digital functions. Here, the portability of services, the reversibility of commitments and the interoperability of formats go beyond the "simple" human costs of migration and, particularly in the cloud, involve technical (proprietary formats and architectures), legal (contractual restrictions without standard clauses, tied sales) and economic barriers (pricing policies with delayed effects, scalable and without medium-term visibility). Services are sometimes offered with no initial costs, or even with credits of several hundred thousand dollars – up to £200,000 for Google Cloud – creating a technical and human dependency that is difficult to reverse. Regulatory progress is being made on this issue, and the Data Act provides for a number of safeguards, including the announced end in January 2027 of the "Too-Big-To-Exit" model, which significantly slowed down data transfer due to egress fees[1].

Furthermore, the combined financial weight of the digital giants gives them an investment capacity in critical infrastructure that neither governments nor incumbent operators can match. Added to this are unrivalled budgets allocated to research and development (Futuribles). For example, GAFAM will invest more than $200 billion in innovation in 2023 alone, compared to $60 billion in France (public and private combined, according to Polytechnique Insights). In both cases, the various successes of the platformisation of the economy enable private digital players to integrate strategic infrastructure into their assets to ensure control of communication channels on a global scale, in a sustainable and diversified manner.

1- Exit fees charged for switching from one cloud provider to another.

The expansion of data centres illustrates this concentration of strategic infrastructure in the hands of players who are, on the one hand, leaders in the cloud software and services market and, on the other hand, key partners of operators of other critical infrastructure such as Internet exchange points. Market leader Amazon (AWS) has grown from 550 "data factories" in 2020 to more than 1,000 in 2024 and plans to operate 3,000 sites by 2030 (ICT Journal). In second place, Microsoft has 120 availability zones, ahead of Google Cloud Platform, Meta Platforms and IBM Cloud.

Major technology players seem to be seeking to absorb carbon-free energy production infrastructure to strengthen the resilience of their data centres. This is evidenced by the proliferation of strategic partnerships in the nuclear sector, such as Microsoft and Constellation Energy, which have relaunched the Three Mile Island power plant, Amazon developing SMR reactors with X-Energy, Google ordering a fleet of molten salt reactors from Kairos Power, and Meta partnering with Constellation Energy in Illinois.

Furthermore, these players are exercising increasing logistical control over digital flows, particularly via submarine cables, which carry more than 95% of intercontinental digital traffic and whose use, mainly for professional purposes, is increasing by an average of 50% per year (IFRI). Admittedly, a few public initiatives at national (Ministry of the Armed Forces), regional (European Commission) and global (BFM) levels are seeking to secure the seabed and diversify digital corridors, but hyperscalers alone already accounted for nearly 65% of global capacity in 2020. Recent strategic projects (Usine Digitale) such as Humboldt between Chile and Australia, Nuvem between the United States and Portugal, and Marea and Sol between the United States and Spain (Microsoft and Meta on the one hand, Google on the other) demonstrate this trend towards increasing private territorialisation of essential infrastructure for the global digital economy.

By 2040,

the planet will therefore be enveloped in an increasingly dense network of data, and few places will escape "ubiquitous and universal" connectivity and the democratization of connected objects. The digital space – including outer space – will also be based on a comparatively much smaller number of physical locations, which will be increasingly tightly controlled by private actors whose very activities are driving this trend. The challenge for professional organizations will therefore be to provide economic support for access to future data storage, processing, and transmission services. For governments, the challenge will be to maintain sufficient sovereign control over critical infrastructure to ensure a fair balance that benefits the common good in the allocation of resources.

Trend 3.

Trend 4. Chinese mega-competitors in B2B digital are maintaining their growth by expanding outside the European market

Over the past decade, China has implemented numerous measures to promote the empowerment of its digital economy through the emergence of national champions and the consolidation of players capable of competing on equal terms with the world's largest competitors. The creation of public investment funds, easier access to credit, and the consolidation of public companies through massive subsidies to support R&D and industrial innovation are all mechanisms through which China supports the growth of its digital players, the acquisition of new technologies and skills, and the development of strategic or emerging markets (semiconductors, biotechnology, robotics, digital twins, telecommunications equipment, 5G, advanced optics, electric vehicles, drones, embedded AI and LiDAR sensors).

Domestically, an assessment of the Made in China 2025 programme (Rhodium Group) reveals the success of a long-term industrial ramp-up strategy based on reducing dependence on strategic imports (electrical equipment, industrial IT, batteries, optical components), pressure on foreign firms to localise their production in China, and restricted market access for certain foreign activities. The desired dual effect was to shape an ecosystem favourable to new players (Alibaba Cloud, CATL, DJI, Inspur, HESAI, RoboSense, Mindray, and now DeepSeek in IAGen, or Kimi from MoonshotLabs and Manus from Monica for local AI), while strengthening the cluster of mega-competitors made up of BATXH (Baidu, Alibaba, Tencent, Xiaomi, Huawei).

In this regard, Huawei's very Chinese "victory without a fight" in the multiple Sino-American tariff escalations demonstrates the acquisition of an unprecedented position. Despite the US restrictions on semiconductors in December 2024, limiting Chinese access to advanced technologies (24 types of equipment banned, BIS licences required), Huawei has turned these obstacles into opportunities[1]. Barred from sourcing and accessing the US market, the company has avoided customs tariffs and is now positioning itself as an alternative to Nvidia in the AI graphics card market. Paradoxically, these restrictions have encouraged the development of local AI models that are less dependent on foreign hardware, just as the loss of the Android operating system and Google services has benefited Huawei's HarmonyOS Next operating system.

Externally, 2025 is also a key date for taking stock of the actions carried out over 10 years as part of the Digital Silk Road (DSR) within the Belt and Road Initiative (BRI) project. A discreet pillar of Chinese technological diplomacy, the DSR embodies a form of restructuring of the global digital economy that not only involves technological breakthroughs but also operates through strategic circumvention and normative diffusion starting from peripheral areas (Council on Foreign Relations).

1- Huawei had already pulled off a similar feat in 2023, offering a smartphone with a 7 nm chip thanks to SMIC, which was also affected by US restrictions in 2020. Although SMIC lags behind TSMC and Samsung (5-3 nm chips), it is supported by a private ecosystem.

Under these conditions, B2B players do not seem to be seeking to conquer European markets head-on through competitive saturation – as in the automotive or photovoltaic equipment sectors – but rather to make progress through margins and circumvention, taking advantage, like DeepSeek, of peripheral relays in Africa, Central Asia, Latin America, the Balkans and the Middle East. These areas, which are often overlooked by Western industrial priorities and are relatively unregulated, are becoming laboratories for an alternative, China-centric digital model based on Chinese infrastructure (cables, 5G, satellites, data centres), proprietary architectures, skills and standards. Although not directly targeted, Europe seems to be concerned about the growing footprint of these companies in its own areas of influence. Forced to be a spectator rather than a participant in direct confrontation, Europe remains powerless to contain Chinese advances beyond its own borders.

By 2040,

extraterritorial sanctions, Sino-American decoupling and the rise of the surveillance economy are likely to encourage Chinese consolidation around the BRICS countries, outside the Western sphere of influence. Chinese digital companies in the B2B segment should no longer suffer from the bottleneck represented by access to cutting-edge equipment (Le Monde informatique), which currently hinders China's ability to take the top spot in the global economy. The maturity acquired by Chinese B2B giants and their positioning on the periphery of the European sphere of influence could then lead to a forced opening of the European market to Chinese digital products and services.

Trend 4.

Trend 5. The emergence of European digital champions offering credible, high-performance and resilient alternatives is supported by initiatives and structuring efforts

The current dynamics of the digital market in Europe are part of a tense period, in which the continent's technological organisation must reposition itself in the face of a globalised landscape largely dominated, at all levels, by non-European suppliers. The emergence of European digital champions is no longer a political communication objective, but an economic necessity for the competitiveness of national economies, requiring the achievement and maintenance of offensive operational resilience. Breaches of supply contracts, such as those that occurred following Broadcom's price increases (Le Monde Informatique), serve as a reminder that service continuity is not guaranteed in an environment of open economic warfare.

The EuroStack initiative represents a significant policy shift in this regard. Defined in February 2025 as a joint industrial roadmap, it aims to structure a "technology stack" based on seven interconnected layers: critical resources (raw materials, energy, water), integrated circuits, networks, connected equipment and objects, cloud, software building blocks, data and artificial intelligence. The stated objective is to build – through a consortium, EDIC Digital Commons – a network of coherent, interoperable and sustainable digital infrastructures capable of guaranteeing functional sovereignty from cable to code. Several hundred European industrial players support this realistic approach of credible, regionally-based alternatives, which makes it possible to coordinate existing assets, activate substantial private investment leverage in the most strategic segments and put in place governance to prevent any form of predation.

The public investments announced reflect a sustained and unusual ambition: €109 billion consolidated under the France 2030 plan, corresponding to a trajectory of private commitments, mainly foreign, revealed at the AI Summit in February 2025, and €200 billion at European level, as part of the InvestAI initiative led by the Commission. Although these budgets are distinct in nature – industrial for France, mixed for the EU – they converge towards the same goal: to structure a sovereign technology sector capable of producing, training and exploiting new-generation models, while strengthening the continent's digital infrastructure. They are aimed in particular at commissioning infrastructure (such as Jupiter) and exascale computing centres[1] (such as Mistral Compute), the creation of regional AI clusters with high capacity density, the creation of centres of excellence to train 100,000 qualified people by 2030, and the deployment of European AI gigafactories with up to 100,000 high-performance chips. At the same time, local technology hubs will enable more precise and controlled use of computational resources by hosting start-ups, laboratories and industrial companies on shared infrastructures designed as alternatives to traditional centralised architectures.

> ***Certain achievements in Europe demonstrate an emerging strategic dynamic across various layers identified by the Eurostack initiative****. France already has Europe's largest sovereign supercomputer, owned by Scaleway, and its equivalent in terms of classified information, owned by Orange. With the "Mistral Compute" project, which positions it in the exclusive club of "exaflop supercomputers", the usual dependence of AI players on the computing power of the cloud should be significantly reduced. This project is based on the deployment of 18,000 NVIDIA GPUs in a 40 to 100 MW data centre in Melun in the Essonne region, which will enable the French company to cover the entire AI life cycle, from model design to deployment, including training, inference and implementation in specific use cases. The use of NVIDIA graphics cards was widespread, but legitimate questions remain about the associated technical risks (backdoors, kill switches) and the stability of hardware supply. At the same time, the start-up VSORA has deployed its Jotun8 AI chip, which is three times more powerful than current standards and consumes half the energy. For its part, Outscale is structuring its sovereign offering around AI, quality and security, in line with the logic of specialised, distributed and interoperable platforms. Other players such as OVH in the cloud segment and La Suite Numérique and Wimi for collaborative suites are reinforcing this dynamic by offering controlled technical environments geared towards critical public and industrial uses. At the international level, Lidl is venturing into software publishing through its subsidiary LSP Digital, and 8Era is developing a 100% modular data centre, optimised for new-generation scalable architectures.*

1- Exascale computing is an improvement in computing capacity, enabling modelling, simulation, AI and data analysis on an exaflop scale, i.e. via a very large number of floating point operations per second.

On a continental scale, the DIGITAL programme for a digital Europe provides structural funding, with more than €8 billion dedicated to supercomputing, AI, cybersecurity, skills and the dissemination of digital uses. It is in line with the Digital Compass for 2030, whose objectives are clear: widespread gigabit connectivity, doubling Europe's share of semiconductors to promote strategic autonomy[1] , deployment of 10,000 secure, low-carbon edge nodes, the first quantum-accelerated computer, adoption of AI and the cloud by 75% of businesses, expansion of funding for unicorns, and increased digitalisation of SMEs.

The European Commission articulates these objectives with the findings of the Leč and Draghi reports. It plans to create a common platform for purchasing critical raw materials, revise public procurement rules to include a European preference through the Buy European Act currently being drafted, and take measures to strengthen national supply chains. The Draghi report recommended, as a priority, a massive investment of €800 billion per year over five years to boost industrial innovation, while the Leč report specifically proposed adding a fifth freedom to the single market, dedicated to the circulation of data, knowledge and skills.

By 2040,

faced with challenges to economic globalisation processes, Europe cannot be satisfied with rhetorical sovereignty or excessive politicisation of this concept. The emergence of genuine strategic autonomy and credible European alternatives could depend on the willingness and ability of public authorities, private actors and investors to foster a cooperative and competitive digital ecosystem at the European level. In order to mature and achieve scale, new European champions should also be able to benefit from the industrial deployment of research and support for the development of their business models until they are listed on the stock market. This approach cannot be part of a strategy to immediately and completely catch up with the United States or China. Instead, it could result from a targeted strategy based on technological and political convergence effects and on certain critical layers. The alternative to the oligopolistic situation would not, therefore, lie in the creation of a gigantic dominant platform, but in the proliferation of European platforms and cross-shareholdings capable of structuring a competitive, integrated, open, transparent and innovation-rich technology market. Structural investment decisions could be based primarily on use cases with the most significant industrial leverage, with the aim of maturing a free, interoperable and sustainable infrastructure. Market conditions could also play a greater role in the ability to control, produce, maintain and develop technological solutions. The new framework of economic conflict based on the triptych of competition, contestation and confrontation may no longer be endured solely to "help the United States maintain its technological advantage" (Ursula Von der Leyen), at the cost of unequal treaties imposing customs tariffs and strategic mass purchases. In this way, European ambitions for autonomy in terms of security, performance and sustainability could be achieved in the most strategic way in the long term, i.e. in a targeted, qualitative and advantageous manner.

Trend 5.

1- It should be noted that ASML is the world's only manufacturer of machines capable of producing the most advanced semiconductors using extreme ultraviolet (EUV) lithography.

Trend 6. The trust market continues to grow

As cyberattacks become more diverse, generative technologies blur the lines between reality and fiction, and artificial intelligence models integrate decision-making into critical systems, one certainty emerges: **digital progress cannot be sustainable without the consolidation of a trust market**. The convergence of technical, legal and ethical issues is now shaping a strategic security economy based on traceability, certification and authenticity. Automated decision support systems, particularly in healthcare, justice and finance, are driving growing demand for trustworthy AI solutions that are verifiable, audited and certified.

This need for trust extends to businesses, which have been weakened by data theft; citizens, who are confronted with deepfakes and fake news; and governments, which are concerned about their sovereignty. This technopolitical requirement is reflected economically in the continued consolidation of the French digital trust sector (ACN), which exceeds €30 billion in activity and 140,000 jobs, with a record added value rate (47%).

The market is structured around three segments: digital security, which accounts for 45% of the market (access control, identification, secure communications, trusted AI, OSINT); software products, which account for 30% (data and equipment cybersecurity, governance, identity management); and services, which account for the remaining 25% (auditing, training, IT outsourcing).
Six French companies are among the ten global leaders, with strong positions in identity management (Thales, Idemia, Docaposte), cybersecurity (Thales, Airbus D&S, Atos Eviden), and secure payments (Worldline).

The stated ambition of players that are SecNumCloud-qualified or in the process of qualifying, such as S3NS (Thales and Google Cloud) and Bleu (Microsoft, Orange and Capgemini), demonstrates a desire to build trust in technical security, regardless of their approach to geopolitical issues. At the same time, the France 2030 plan and the "Je choisis la French Tech" initiative are supporting the maturation of the national industrial fabric.

In 2024, the government reinforced this approach with the SREN law, which requires the use of certified cloud solutions for processing sensitive data, and in 2025 it renewed its public procurement policy favouring sovereign offerings (public actors). Since June 2025, any acquisition of a cloud solution by a ministry must be validated in advance by DINUM, except in exceptional cases. This strategic line is extended by the mobilisation of the Strategic Sector Contract (CSF) "Trusted Software and Digital Solutions".

By 2040,

the digital trust market should cease to be a technical sector and become the invisible infrastructure of operational resilience. Its growth would be less a consequence of a need than a condition for legitimate progress in a world of heightened risks. As digital technologies are at the heart of a growing number of activities, it goes without saying that the trust placed in them should be a major social issue to be taken into account as importantly as the ethical development of digital technologies themselves.

Trend 6.

Trend 7. The growing influence of regional legislation in the regulation of digital activities raises questions about innovation and operational capabilities

The legal framework for digital activities, long dominated by national or international legislation, has been marked over the last decade by the rise of exclusive regional regulations that have a restrictive and differentiating effect on the operational capabilities of digital players.

There is a shift towards regulations that are not only regionalised but also asymmetrical, as evidenced by the US administration's decision on 10 February 2025 to suspend the Foreign Corrupt Practices Act (FCPA) for a period of 180 days. By temporarily removing a fundamental instrument for combating corruption in international commercial transactions, the United States is strengthening its capacity to capture certain markets while maintaining judicial pressure on European companies. As such, the cumulative total of sanctions imposed to date on players such as Airbus, Alcatel, Alstom, Total, Safran and Société Générale exceeds $5 billion, not counting ongoing extraterritorial investigations, while US players benefit from a regime of apparent neutrality. Similarly, on 21 February 2025, President Trump signed a memorandum explicitly targeting the European Union's technology regulations (Digital Markets Act, Digital Services Act), which he described as regulatory extortion. This text, which went relatively unnoticed, is in fact a strategic statement that the United States intends to oppose European ambitions to regulate platforms with its own normative legitimacy. The announced suspension of certain tax and customs cooperation, notably through the imposition of tariffs on digital services, could call into question the previously negotiated balances – as evidenced by Canada's early repeal of its digital services tax as part of bilateral negotiations with Washington in June 2025.

The pressure of regional regulations is not only exerted on taxation or anti-competitive practices, but now extends to infrastructure and data regimes. The battle for raw materials, critical equipment and cross-border flows is compounded by legal disputes over the location, portability and exploitation of data. The decision by the Irish Data Protection Authority to fine TikTok €530 million for illegally transferring data to China is a significant example of this. The sanctions imposed by the French data protection authority CNIL on Google (€525 million for illegal prospecting on Gmail) also illustrate the rise of restrictive territorial regulation, which could no longer be limited to the principles of the GDPR but would enter into a logic of decentralised technical sovereignty.

European regulation is no exception to this complex interaction between territorial levels. The postponement of the vote on the EUCS certification project for cloud services, requested by France due to differences with its own SecNumCloud standard, demonstrates the internal tensions surrounding the definition of cybersecurity standards. Complexity also arises from the interactions between different regulations such as the AI Act, the DMA and the GDPR, which are the subject of simplification projects (Challenges) whose guidelines should clarify their respective articulations and scopes for the benefit of innovation and European economic activity.

In terms of competition, the proceedings brought against Apple, Google, Amazon and Microsoft all target their market power and their ability to lock down strategic business segments. The conditions imposed by the Apple Store, the mechanisms of algorithmic favouritism on Amazon, and the difficulty of migrating between cloud offerings at Microsoft constitute a set of barriers to innovation and market fluidity, which are prompting growing mobilisation by local judicial authorities in the United Kingdom, the United States and several EU Member States. For example, the May 2025 ruling in Epic Games v. Apple, authorising third-party payment methods, resulted in an immediate modification of the Spotify app, allowing it to bypass Apple's proprietary system and avoid the nearly 30% commission imposed on subscriptions made through the App Store.

By 2040,

regional regulations could become even more strategically significant, going far beyond the simple legal framework of compliance. With the aim of serving their stakeholders, their digital market and their capacity for innovation as much as possible and in a realistic manner, these regional regulations could take on a more offensive character and represent a strong political, economic and civilisational marker. In the European case, while the NIS2, DORA, EUCS and the Cybersecurity Act currently accompany the reduction of vulnerabilities with defensive resilience, offensive texts such as the DSA, DMA, Data Act and DGA could in future be the founding elements of a model of "good ethical behaviour" that could be projected into the grey areas of global cyberspace (Africa, the Balkans, Southeast Asia). This normative movement would also reflect a political will to go beyond the defence of European consumers to structure markets according to a clarified purpose, taking into account the needs of European producers of digital goods and services. Regulatory bodies would thus become, in certain territories, geo-economic actors in their own right – acting as arbiters of balance, guarantors of fundamental rights, and strategists of distributed sovereignty. However, this role could only be fully assumed if these standards were accompanied by an explicit industrial project and a strategy for extensive cooperation and concrete support for the legal framework of local businesses.

Trend 7.

Hypotheses of disruption by 2040

1. The American tech sector generates a new financial bubble that eventually implodes.
The frantic race for technological innovation – fuelled by massive investments in AI, semiconductors, space and cloud infrastructure – could create a new financial bubble. Dependence on financial markets and rising energy and logistics costs could weaken the American digital giants. A growing gap between financial valuations and actual revenues generated, investments made and profitability achieved could lead to the bursting of a financial bubble similar to that of the Internet. A crisis in business models and a breakdown in investor confidence could lead to a reconfiguration of global technological leadership, benefiting more sober or regionalised players (Asian or European) focused on qualitative rather than quantitative metrics.

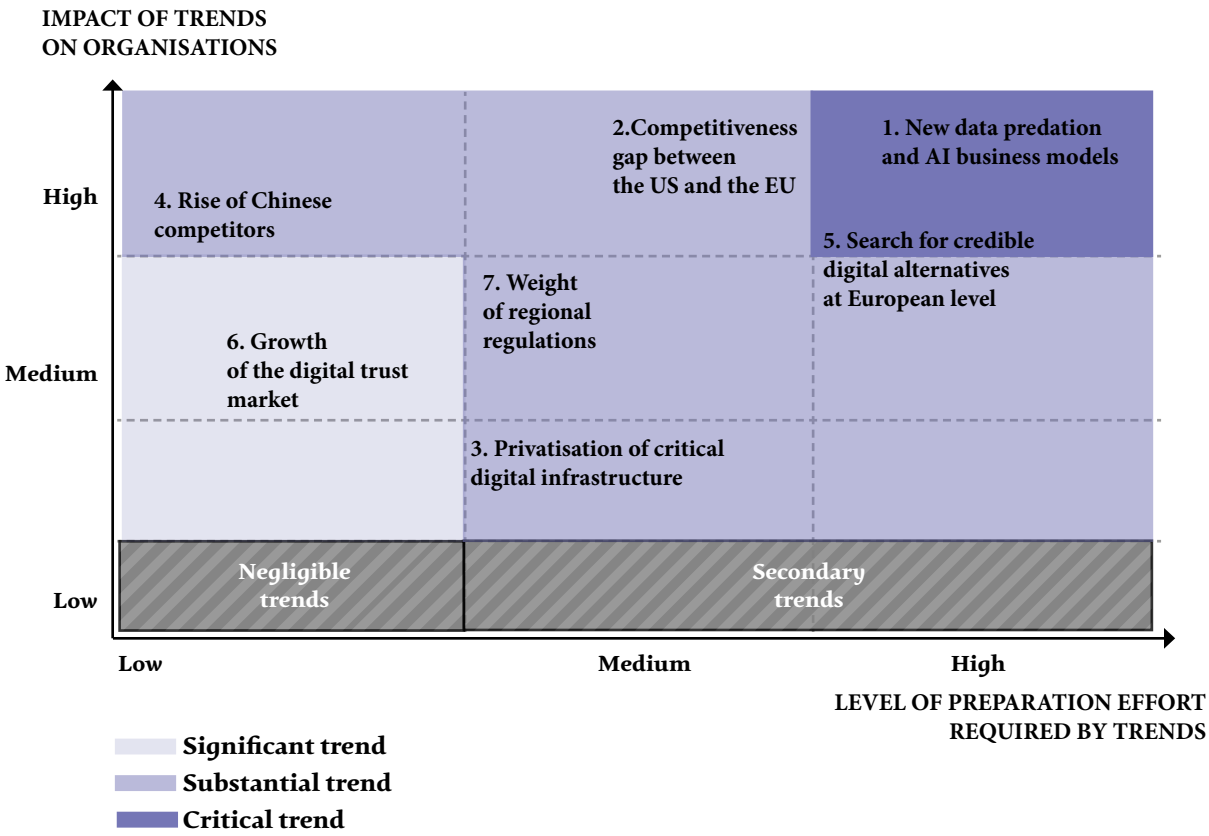
2. Europe is unifying its digital services market. European digital champions are emerging and becoming indispensable in strategic value chains.
After decades of fragmentation, the European Union could succeed in harmonising the various legislative provisions, critical infrastructures and industrial policies within its borders to support a single market for digital services. Through political will and the strategic interests of stakeholders, several European organisations could take advantage of this unprecedented alignment to achieve critical mass, establish a new benchmark for globally essential offerings, and strengthen regional resilience in several critical digital segments.

3. Trusted digital technology enables payment, identity and health data to be pooled in a European "super wallet".
By 2040, the ubiquity of digital wallets[1] in social interactions could lead to a convergence of digital services around a European public application based on the principle of identity and authenticated data federation (IADF). This European "Super App" could enable citizens to manage their identity, payments and assets (real estate, savings, cryptocurrency, professional, etc.), health data and administrative procedures in a fluid and unified environment. It could be a means of rebalancing the weight of European digital sovereignty in the face of predatory practices by non-European private consortia, while raising major issues of governance, interoperability and transparent protection of individual freedoms.

1- Electronic wallets primarily provide a secure information storage service. They are used in particular as a means of payment (storage of bank card details, accounts, gift cards and loyalty cards, discount vouchers) or as administrative documents (storage of driving licences, transport tickets, event tickets or identity documents).

Summary
Field 02 –Digital Economy

Major trends effort matrix



Reminder of the assumptions for disruptions by 2040

1. The American tech sector generates a new financial bubble that eventually implodes.
2. Europe unifies its digital services market. European digital champions emerge and become indispensable in strategic value chains.
3. Trusted digital technology enables payment, identity and health data to be pooled in a European "super wallet".

Field 03

Technology & Innovation

Major trends and disruptive hypotheses

Major trends

Trend 1. The three pillars of the cloud – computing power, storage, and networking–remain at the heart of the competition for innovation

The race for digital innovation relies heavily on optimising the three fundamental pillars of the cloud: computing power, storage capacity and network infrastructure performance. These elements form the technical backbone of the digital economy, and their evolution is shaping the contours of a contested technological hegemony.

In terms of computing power, exascale architectures[1] accelerate the industrialisation of artificial intelligence, particularly with the deployment of Nvidia Blackwell B200 GPUs[2], capable of reaching 100 teraFLOPS per unit, which is comparable to the computing power of supercomputers from the previous decade. Mistral Compute, in France, has deployed 18,000 GPUs of this type in a data centre in Essonne, providing a theoretical capacity of 50 exaFLOPS[3].

1- Exascale computing refers to a level of advanced computing capable of performing at least one exaFLOPS of floating point calculations per second. It enables the advanced use of converged modelling, simulation, AI and analytics technologies.
2- A GPU is a graphics processing unit, i.e. an electronic circuit. It was largely designed to reduce the time needed for a computer to run multiple programmes. The ability of GPUs to perform a large number of calculations or tasks simultaneously through parallel processing makes them faster and more efficient than the CPUs of older computers.
3- FLOPS are a unit of measurement for the computing speed of an IT system and therefore part of its performance. They refer to the number of floating-point operations performed per second.

These high-performance infrastructures, powered in part by carbon-free energy, enable language models to be trained, critical industrial scenarios to be simulated and complex computational tasks to be performed in real time. Disaggregated "compute S storage" architectures, meanwhile, enhance operational efficiency by dynamically separating workloads according to business and sector needs.

In terms of storage, technologies are evolving towards high-density formats with a low energy footprint. Molecular storage on DNA, tested by Biomemory and supported by research conducted by the CNRS and Sorbonne University, paves the way for long-term data storage without an internet connection (Cold Storage[1]), for massive volumes, with energy consumption up to a thousand times lower than that of conventional disks (CNRS Innovation). At the same time, NVMe-over-Fabrics[2] formats coupled with PCIe Gen5 SSDs[3] enable speeds of over 14 GB/s and latency of less than 100 microseconds, making computing and AI infrastructures more agile and responsive. Synthetic storage and ZNS (Zone NameSpace) formats, which are still rarely used on a large scale, reduce fragmentation and optimise data flows in hyperscale[4] environments, with enhanced interoperability between public clouds and local infrastructures.

In terms of network infrastructure, the convergence of telecoms networks, the cloud and edge computing is accelerating as a result of virtualisation and the integration of AI into radio resource management. The development of 6G, currently in the pilot phase in several European research centres, promises latency of less than a millisecond and a theoretical speed of 1 Tb/s, while low-orbit satellite networks are taking on a strategic role in areas not covered by fibre or relay antennas. The development of infrastructure such as Iris², a satellite constellation project overseen by the European Commission and designed to provide secure and resilient connectivity, could reflect an effort to achieve autonomy and sovereignty in the management of tomorrow's telecommunications networks.

By 2040,

the targeted, secure, and more energy-efficient orchestration of cloud technologies should reinforce the development of strategies for interoperability and financial control of associated expenses. These technical foundations for organizational data should determine the industrialization of AI, resilience to cyber threats, and the ability to structure independent digital infrastructures adapted to critical use cases. Mastering these foundations should continue to be a priority for public and private action.

Trend 1.

1- The term Cold Storage refers to a method of storing private keys, which allows them to be held and stored on an offline medium, without being connected to the Internet.
2- "Extension of the NVMe network protocol for Ethernet and Fibre Channel systems, which accelerates and strengthens connectivity between storage solutions an- servers, and reduces the load on application host server processors." - Purestorage, 2025, What is NVMe over Fabrics (NVMe-oF)?
3- "PCIe Gen5 NVMe SSDs (solid state drives) are the latest improvement and are setting the new standard for high-performance storage. While maintaining backward compatibility with other PCIe slots, PCIe 5.0 SSDs offer speeds up to twice as fast as 4.0 SSDs. " - Kingston, July 2025, What is a PCIe Gen5 SSD?
4- "The ability of a system or technology architecture to scale as demand for resources increases." - Fortinet

Trend 2. AI technologies are proliferating and are set to transform activities far beyond the digital ecosystem alone

For nearly a century, research into artificial intelligence has evolved alongside the rise of digital technology. But since 2023, with the general public's access to large generative language models (IAGen), the promises have become more pressing than ever, with some heralding the wave of productivity so eagerly awaited by the digital sector, and others facilitating processes and faster, more informed decision-making.

> *Behind the promises of productivity gains and process optimisation (McKinsey), it is essential to distinguish three main strata within AI technologies.*
> ***Firstly, AI systems[1] refer to the overall architecture** that brings together hardware components (GPUs, TPUs, DPUs), software components (computing frameworks, orchestrators), and interfaces (APIs, business portals) to provide automated or semi-automated computational functionalities.*
> ***Secondly, AI models constitute the mathematical and statistical substrate of AI technologies**. Shared mainly between neural networks, large language models (LLMs), large vision models (LVMs), and large action models (LAMs), they are trained on large volumes of varied data, using machine learning or deep learning techniques, and define the ability of AI to perceive, interpret, predict and act. Their enrichment with higher quality data and shorter retraining cycles is one of the potential disruptions in this value chain.*
> ***Thirdly, AI functions correspond to the intended use of these systems and models**. They respond equally well to analytical uses (collection and preparation of data for predictive analysis or emotional analysis, etc.) and generative uses (text, image, video, code, music, etc.) or "algorithmic" decision-making uses (planning and execution of autonomous sequences of actions in dynamic environments), with a strong potential to disrupt the digital space.*

The number of developments underway in AI and the proliferation of innovations are staggering. The economic impact of each of these technological strata extends far beyond the digital ecosystem alone. Global competition in this area of technology is extremely fierce and takes place at every stage of the AI value chain, from the physical infrastructure required for AI technologies (energy, multiple hardware devices, connectivity and computing), to the software structure (algorithms used), the integration of AI into existing information system architectures, the security of applications, the quality control of data produced by the technology, and the referencing of AI tools (Usine Digitale).

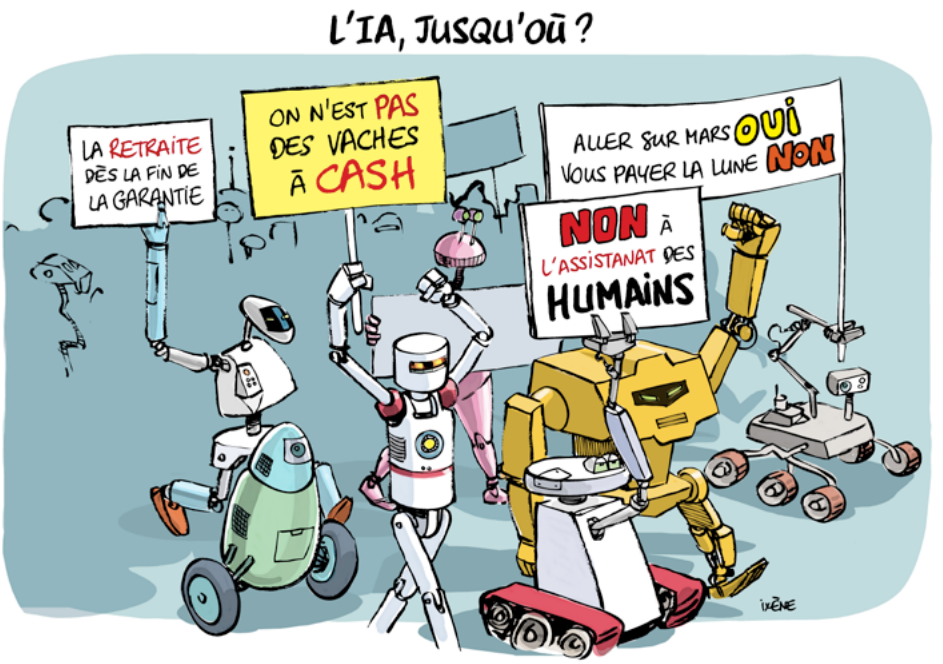
1- According to the definition in the European AI Act: "An AI system" is a machine-based system that is designed to operate with varying levels of autonomy and can demonstrate adaptability after deployment, and which, for explicit or implicit purposes, infers from the data it receives how to generate outputs such as predictions, content, recommendations or decisions that may influence physical or virtual environments.

The technological buzz surrounding AI has reignited the race to control infrastructure. One example of this is the major American Stargate project, which brings together OpenAI, Microsoft, Oracle and MGX to build 50 mega data centres dedicated to AI, financed to the tune of $500 billion by SofiBank and BlackRock. Another example is France's response at the AI Action Summit, announcing a €100 billion investment in the construction of "mega data centres" and the opening of Europe's largest AI campus. Finally, to name but a few examples, there is the European call for Made in Europe initiatives, "EU AI Champions", with €200 billion to develop the world's largest public-private partnership in this field, and the "Invest AI" project, with more than €20 billion mainly dedicated to the integration of AI in "Gigafactories".

The technical requirements of the cloud for cutting-edge AI applications are such that they make it a major strategic lever for innovation. The historic agreements signed between Saudi Arabia and the United States in mid-May 2025 – involving cross-investments and supplies from Nvidia, AMD, AWS, Google, Data Volt, etc., worth more than $100 billion – are a strong signal of a new set of digital alliances (Reuters). Thus, in the same way that rare earths were considered as a bargaining chip in the peace negotiations related to the Ukrainian conflict, GPU resources and storage, computing and network capacities for the cloud and AI are becoming a credible diplomatic alternative to traditional oil contracts.

Competition at the algorithmic level is no less intens*e*, and China is raising fears of an "Sputnik moment" for AI: despite chip embargoes, Liang Wenfeng's DeepSeek model is said to offer performance comparable to that of OpenAI for an investment of between $500 million and $1 billion (Le Grand Continent). The Deepseek model's distinctive choice in favour of hybrid architectures, which are specialised and therefore more computationally efficient, fuels criticism of the sustainability of the universal LLM model (Le Grand Continent). This standoff between hyperscalers and national challengers is taking place within a regulatory framework that is undergoing a complete overhaul. The European AI Act, which came into force in February 2025[1], establishes an initial legal framework aimed at European uniformity for the development, marketing, commissioning and use of artificial intelligence solutions. It concerns all players in the AI value chain (suppliers, deployers, agents, importers and distributors) operating in Europe. The aim is to manage the deployment of AI according to four levels of risk (from unacceptable to minimal), while seeking to compromise neither the spirit of innovation nor European fundamentals. **The AI Act responds to a strong need for built-in guarantees: transparency** (in real time on systems put into production) **and explainability**, specific to models or applied after training and adapted to the particular needs of different users. Without addressing the issue of digital trust here, the establishment of a balanced framework for use that goes beyond the legal obligations for so-called "High risk" has emerged as a sine qua non condition for ensuring the ethical development of AI in organisations, and is one of the key conclusions of the Summit for Action on Artificial Intelligence co-chaired by France and India in February 2025.

1- The Commission also plans to introduce legislation on cloud and AI development, with an action plan for the creation of AI factories in the first quarter and the presentation of its "Strategy for Applying Innovation to AI" in the third quarter.



At the same time, agentic AI promises such advanced automation that it could play the role of a fully functional entity, from autonomous commerce (PayPal is already preparing its "agents") to fully automated predictive maintenance, interaction with business systems and database management. Numerous applications are being developed for the agentic function, including the self-improvement of chatbots based on past conversations, personalised recommendations in e-commerce, streaming, educational content and the continuous management of numerous organisational processes. **These agents, orchestrated by protocols such as Anthropic's MCP or Google's first agent-to-agent standards, will become as crucial to agentic AI as APIs have been to the development of web applications.**

Through these various channels, artificial intelligence technologies and innovations are now penetrating sectors that were once considered out of reach (Cigref): healthcare is using immersive teleconsultation and agentic AI for disease detection and treatment development, defence is deploying autonomous drones guided by computer vision, Industry 4.0 orchestrates its production lines in real time and designs its prototypes using digital twins, the financial sector refines its scoring and anti-fraud models, the energy sector adjusts its smart grids, transport improves the possibilities of autonomous driving, public policy makers find it easier to carry out impact studies, and administrations find it simpler to generate personalised documents. AI is no longer limited to the digital ecosystem and is redefining the trajectory of many sectors in different ways, requiring a profound cultural transformation and imposing an unprecedented alliance between engineering, regulation and ethics to ensure secure, responsible and sustainable co-construction.

By 2040,

the production of synthetic data by AI could become a key resource in industry, enabling certain companies to become veritable "AI factories" through data production. Regardless of the field (industrial, financial, healthcare, agricultural, defence, space), each entity could be capable of operating its own AI engine, fed and configured with its activity history. The convergence of local data, intelligent APIs and specialised models should also spell the end of LLM models for generative use by the general public. In this new digital landscape, decision-making flows themselves should be largely co-optimised by AI agents and orchestrated with almost organic finesse.

Strengthening data governance may no longer be seen as a precautionary measure, but as a strategic discipline in its own right: the ability to trace the origin of models, document their training, audit their biases or continuously certify the nature of data (human or synthetic) will all be levers for a renewed form of algorithmic resilience. Without these private safeguards and without a fair and balanced policy framework, systemic risks (hallucinations, biases, sensitive leaks, energy rebounds) could fully compromise the gains achieved.

In this context, APIs should be to digital and cognitive functions what supply chains are to physical goods. Orchestration platforms should therefore become the nerve centres of a reshaped digital economy, where "AI pipelines" will be embedded in multi-level architectures, right down to the end consumer. Organisations that are able to combine mastered generative and agentic AI, ethical data governance, human, hardware and software expertise, while promoting synergies with the robotic layer, should be the true pioneers of the new industrial era that is dawning.

Trend 2.

Trend 3. Public and private players are preparing for the emergence of quantum technology

Quantum computing appears to be the third major breakthrough in computing power, alongside the widespread adoption of cloud computing and the explosion of artificial intelligence. Its promise of unrivalled computing power to solve complex problems is already sparking a strategic and legislative race across the five major stages of the quantum value chain: fundamental research, manufacturing of enabling technologies (electronics, telecommunications, photonics, cryogenics, lasers, rare materials, etc.), equipment manufacturing (sensors and measuring instruments, communication networks and quantum computers), development of solutions and services (quantum computing, telecommunications and cryptography, metrology) and deployment (energy, healthcare, defence, etc.). etc.), equipment manufacturing (sensors and measuring instruments, communication networks and quantum computers), development of solutions and services (quantum computing, telecommunications and cryptography, metrology) and deployment of applications and business services (simulation, optimisation, cryptography and machine learning based on innovations in AI).

Governments and manufacturers are already organising major research and development programmes in quantum computing, based on at least two complementary approaches: defensive resilience, to avoid suffering the multiple consequences of this wave of technological innovations to come, particularly in terms of security, and proactive resilience, to make the most of these applications to achieve tenfold performance gains. The still experimental segment of quantum computing includes technologies specific to quantum computers (control of qubit entanglement[1] via quantum gates of their coherence[2]) and quantum simulators.

> ***At the national level, France has reaffirmed its ambition to develop quantum computing by allocating more than €1 billion to its national programme "France Quantique" (Info Gouv) for 2025-2020****, while Germany plans to spend nearly €1 billion to develop a sovereign quantum computer (Euractiv). Intellectual property regimes, public-private partnerships and the creation of the European Quantum Industrial Alliance are becoming key levers for digital resilience, which depends on the autonomy of qubits as well as the security of future quantum computers.*
>
> ***At the regional level, the European Union is launching a new strategy, the Quantum Europe Strategy (European Commission), aimed at creating a resilient, sovereign ecosystem focused on quantum industrial production by 2030****. This roadmap is based on four pillars: strengthening public-private partnerships in research and innovation (Quantum Flagship, Horizon Europe), deploying shared quantum infrastructures (such as a pilot European quantum internet and a secure communication network), consolidating the industrial ecosystem (quantum chip manufacturing), encouraging the dual use of quantum technologies (civil and military) and developing a pool of skills through training. The European Quantum Act, planned for 2025, will aim to coordinate research efforts, protect European patents and prevent the acquisition of emerging technologies by non-European players.*

By 2040,

Quantum computing could reach a decisive milestone, with substantially more widespread sectoral use cases (BCG) in the fields of health, defence and space, chemistry and agriculture, finance, mobility and geology. The global market could exceed €150 billion (Les Echos) and generate thousands of highly skilled jobs. Europe must consolidate its sector, or risk remaining dependent on cloud giants who may be tempted to increasingly restrict access to quantum resources via, for example, Sycamore for Google, Azure Quantum for Microsoft or AI Research SuperCluster for Meta. The value of the first major wave of uses will be captured by players capable of combining hardware excellence and software expertise, in particular by integrating quantum computing in a hybrid manner into architectures already profoundly modified by agentic AI, while resiliently guaranteeing post-quantum security. The first quantum confidential computing services, still in the prototype stage today, could protect sensitive algorithms from emerging computational threats. Intensive training, the development of quantum programming skills, and user-supplier partnerships will be key to making the most of this strategic technological shift.

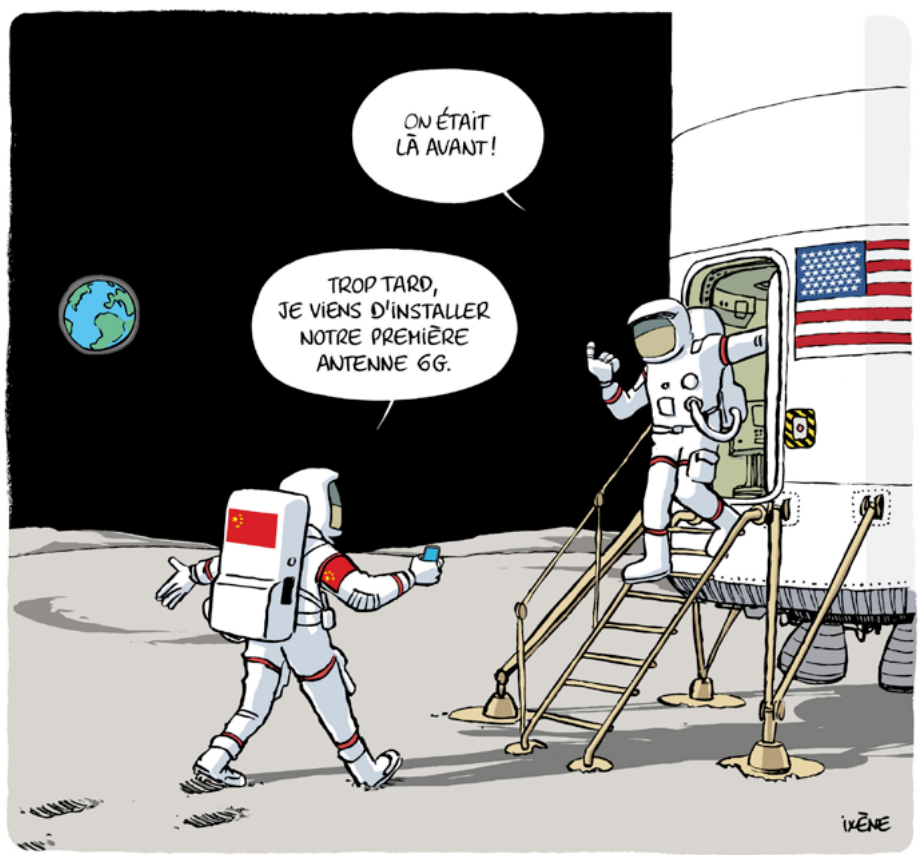
Trend 3.

1- Entanglement is a phenomenon in which two qubits become linked in such a way that the state of one instantly depends on the other, even at a distance.
2- The length of time during which a qubit can maintain its quantum state and perform parallel calculations.

Trend 4. Technological monopoly in space is increasingly coveted

The space sector is becoming a key area of global technological competition, driven by the combined effects of the rise of private initiatives, geopolitical restructuring and a certain upheaval in traditional industrial balances. Far from the cooperative model inherited from the early decades of space exploration, the orbital order is now establishing itself as an area of technological capture and strategic affirmation, where leadership and sovereignty are increasingly coveted.

Space, historically the preserve of states, and more specifically of a handful of major powers with public research and defence agencies, is now increasingly being taken over by industrial consortia and digital entrepreneurs seeking to impose new standards. This phenomenon, known as "New Space", has been growing in importance every year for more than a decade (IHEDN), and continues to drive technological innovation, particularly through the production of private offerings (reusable launchers and rockets, miniature satellites carrying software and telecommunications services, space tourism and Mars exploration projects) affecting many sectors of activity through their use cases (telecommunications, defence, navigation, resource management, meteorology and natural risk monitoring).



> *This shift is mainly reflected in the exponential growth in the number of satellites currently in low Earth orbit, approximately 550 kilometres above the Earth[1]. In the space of ten years, the number of active satellites has increased tenfold (Statista). The private company SpaceX alone operates more than 7,700 active satellites out of the 8,900 launched to date via its Starlink constellation. The company plans to expand to 40,000 units to serve the global market for secure communications and data transmission. Amazon, with its $10 billion Kuiper project (Les Echos), plans to deploy a constellation of 200 satellites and begin marketing its services by the end of the decade. while the Chinese group SSST (Statista) plans to launch 15,000 units for its Qianfan constellation by 2020, and Geespace, a subsidiary of Chinese car manufacturer Geely, is preparing to launch 1,000. The Chinese government, for its part, has launched a satellite constellation project, Guowang, comprising 1,000 satellites. All these deployments are aimed simultaneously at civil, military and commercial uses, with a common technological promise: the provision of global, very high-speed internet access.*

Europe, which has been lagging behind until now, is structuring an industrial response through capital and operational levers (Polytechnique Insights). **At the national leve**l, the French government has taken a 29.99% stake in Eutelsat, which became the leading European operator after the acquisition of OneWeb[2], in a clear move towards sovereignty (Challenges). It should be noted that Eutelsat now has the world's second largest fleet of integrated low-orbit and geostationary satellites, with nearly 600 units operational and capable of being deployed in the Russian-Ukrainian conflict zone (La Lettre). France also maintains its leadership at European level by drawing on the joint work of the CNES and its internal industrial and academic ecosystem. **At the European level**, the Iris² project, supported by the European Commission (Polytechnique Insights), plans to deploy 300 satellites within a secure and resilient institutional framework centred on the SpaceRISE consortium (La Rem) to ensure the continent's sovereign connectivity.

Space is not only a commercial issue, it is also the scene of technological conflict. This is evidenced by the malicious orbital manoeuvres identified by Space Command, the development of military capabilities (patrol satellites, electromagnetic jamming, manoeuvring satellites), projects such as the PWSA (Proliferated Warfighting Space Architecture) of the US Space Development Agency, and the Starshield military constellation, developed by SpaceX on behalf of the US Department of Defence. In addition, the Golden Dome programme is publicly reviving the prospects for offensive orbital weaponry (Reuters), in a logic similar to the American IDS project, or "Star Wars" of the 1980s. In March 2025, the Trump administration's threat (Le Grand Continent) to suspend Starlink connectivity in Ukraine, in response to Russian countermeasures involving jamming and rerouting of communications, highlighted the weight of these new technological dependencies.

1- Low Earth orbit satellites orbit approximately 550 kilometres above the Earth, unlike geostationary satellites, which are positioned more than 35,000 kilometres above the Earth and traditionally provided internet connections in areas without coverage.
2- OneWeb was a British company specialising in low Earth orbit (LEO) satellite telecommunications, while Eutelsat Communications was one of the world's leading operators of geostationary satellites (GEO).

Faced with this infrastructure race, regulatory and legal balances are fragile and sometimes poorly respected, even though the common good of "space" is not legally defined. No treaty sets the boundary between airspace and outer space. Furthermore, satellite frequencies – the number of which is limited by physical constraints – are allocated by the International Telecommunication Union (a UN agency) on a first-come, first-served basis, which partly explains this "space rush" worthy of the Wild West (National Geographic). Furthermore, safety rules remain fragmented, and the massive occupation of orbits – particularly by private constellations – increases the risk of collisions, the production of dangerous debris and spectral saturation. Europe plans to respond with regulations in the coming months through a European Space Act, which would aim to limit commercial uses deemed unreasonable, harmonise technical standards, and prevent extraterritorial capture of bandwidth and orbital space.

By 2040,

space will have become a critical layer in its own right in the mapping of global digital infrastructure, with more than 100,000 satellites in orbit. The satellite industry could become highly attractive – albeit with an increasingly high entry price in a market undergoing consolidation – due to the growing development of new or alternative uses such as data transfer for autonomous vehicles, sat-to-cell services for mobile terminals, and secure coverage in areas without fibre or 5G, particularly in Africa (IFRI). The issue will then no longer be one of a one-off technological comeback, but of full-fledged capacity governance. Coordinated industrial management, consolidated legal regulation and a controlled interoperability model will be the minimum conditions for preserving European autonomy in a space that has become contested and saturated.

Trend 4.

Trend 5. The search for balance between collaborative spaces and secure data is intensifying

In a context where digital collaboration is becoming increasingly widespread, securing sensitive data is increasingly seen as an essential condition for the activity of various organisations, both for the digital trust it establishes and for the sovereign control of the tools and information it may involve. Collaborative work platforms are evolving to offer customers complete control over the location, encryption and access to their information, whether it be documents, databases or personal identifiers.

At the national level in France, the Interministerial Digital Directorate (DINUM) recently developed the "Digital Suite", a set of free software *designed for administrations and already in use by 100,000 civil servants. Built in collaboration with German and American teams, this platform guarantees interoperability, decentralisation and traceability of access, without ever resorting to proprietary code. The forthcoming creation of the European Data and Infrastructure Consortium (EDIC) will ensure the assembly of these open source building blocks.*

Industrial partnerships are also offering secure collaborative suites*. Thalès, in partnership with Wimi, has launched a sovereign platform dedicated to the 2,500 companies in the Defence Industrial and Technological Base (BITD). Certified for use at Secret level, this solution incorporates session locking, sharing control and revision traceability mechanisms that meet the most stringent security requirements. For its part, Docaposte, the digital subsidiary of La Poste Group, has also chosen Wimi to offer local authorities and SMEs a sovereign collaborative platform that complies with GDPR standards, is HDS certified and has SecNumCloud certification, guaranteeing the confidentiality and integrity of exchanges.*

At the same time, privacy-enhancing technologies (PETs) are gaining ground*. Homomorphic encryption, secure multi-party computation and zero-knowledge proofs now make it possible to perform analyses and processing on encrypted data without ever exposing the content to unauthorised parties. These approaches are particularly popular for sharing sensitive data between companies or coordinating urban crisis units, contexts where confidentiality remains imperative (confidential computing).*

By 2040,

the balance between open collaborative spaces and security guarantees will be a marker of resilience on the one hand, and digital sovereignty on the other. It will be based on a combination of interoperable open platforms, sovereign cloud services and advanced cryptographic technologies, enabling each organisation to collaborate on a large scale while retaining control over its information assets.

Trend 5.

Trend 6. The continuum between the real and the virtual is becoming more fluid

The boundary between the physical and digital worlds is blurring under the influence of immersive technologies. Virtual reality, augmented reality and digital twins are transforming collaboration, training and industrial process optimisation. They enable interactive and immersive experiences; however, their deployment remains hampered by high acquisition costs, cybersecurity issues and a shortage of specialised skills.

The introduction of emotional artificial intelligence and humanoids marks a new stage in this continuum. Interactive voice and visual interfaces, combined with real-time processing of feelings and facial expressions, are paving the way for autonomous avatars capable of natural and empathetic interaction. These hybrid robots, born of the convergence of AI and robotics, embody what some are already calling 'agentic artificial intelligence' applied to immersive environments.

> *Among the notable innovations, the "Android XR" prototype illustrates the fluidity of the co-living space. Based on augmented reality technologies, it integrates microphones, speakers, camera and miniature screen, allowing users to ask questions in their native language, capture their surroundings, send an email or create an event, all without taking out their smartphone. It translates foreign languages in real time and guides the user with integrated Google Maps. Unveiled at Google I/O 2024 under the name "Project Astra", this new device has advanced capabilities. Compared to Meta's Ray-Ban, which focuses on miniaturisation and integration with Facebook Horizon, these innovations raise the question of which ecosystem is best suited to dominate the market for tomorrow's glasses.*

By 2040,

the continuum between the real world and the virtual world will become more fluid, potentially leading to the gradual abolition of boundaries between physical interactions and immersive experiences. This sensory and cognitive hybridisation should involve a reconfiguration of the architecture of digital functions to enable real-time orchestration of data flows between embedded terminals, cloud gateways, agentic AI platforms and a variety of interactive and immersive environments. Securing this new space for exchange will rely on demanding pillars such as the local generation of encryption keys in sensitive virtual environments and the adoption of open standards to ensure interoperability between different digital spaces. This dynamic should also accelerate the integration of detailed traceability processes for human-machine interactions, in order to to ensure the trust, integrity and resilience of these augmented collaboration spaces.

Trend 6.

Hypotheses of disruption by 2040

1. Industrial-scale quantum computing is available.
The first generation of quantum computers is already in operation in 2025, with a limited number of applications and users. By 2040, the emergence of the first very large-scale supercomputing offering could represent a tipping point as significant as the release of ChatGPT at the end of 2022. The advent of this technological breakthrough could accelerate the race for computing power and profoundly reconfigure business models, security protocols and innovation methods.

2. The massive deployment of 6G networks and the widespread adoption of Open RAN[1] are profoundly transforming connectivity and telecommunications networks.
The convergence of telecommunications, cloud computing and artificial intelligence could transform networks into segmented, dynamic platforms that can be adapted to demand. The race for faster and more reliable connections is likely to spark a new battle between, on the one hand, new players specialising in virtualisation and cloud computing in the telecoms market (Cigref) and, on the other hand, traditional players in the sector who may try to capitalise on their current advantages (infrastructure, geographical proximity, etc.) to become major players in virtualisation and cloud computing (L'Usine Digitale).

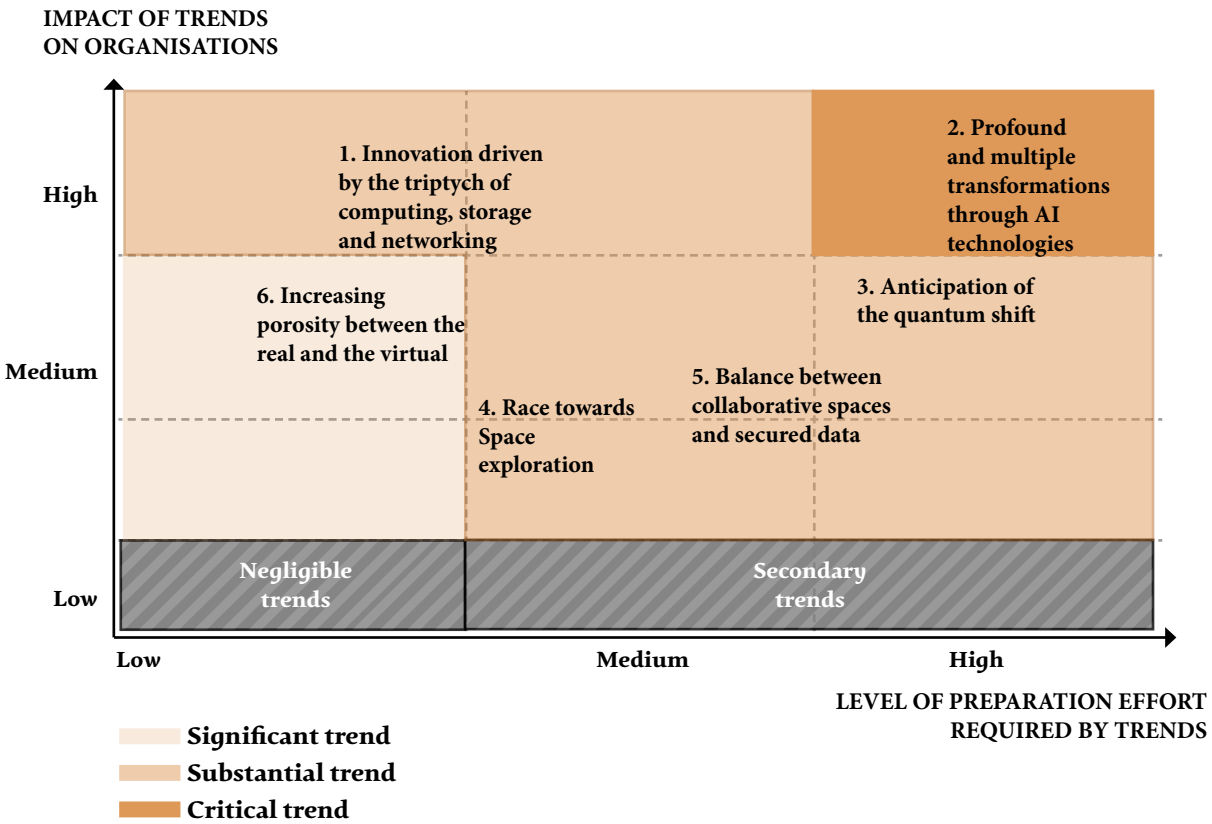
3. Agentic AI is disrupting a considerable number of websites, software programmes and digital tools beyond the professional world.
The widespread use of agentic AI, capable of making complex decisions autonomously in all types of environments, could profoundly transform digital and social environments. Their native integration into operating systems, web platforms and business software could transform every individual, in both their professional and private lives, into producers of their own data industry and managers of AI, even without their knowledge. The super-orchestration of tasks, flows and interactions without direct human intervention could render many traditional tools obsolete, redefine human-machine interfaces and outsourcing logic, and raise new questions about the traceability of decisions, algorithmic responsibility and the governance of autonomous systems.

4. The first General AI is created.
The creation of a general AI capable of performing all human intellectual operations in a completely autonomous manner would constitute a civilisational breakthrough. The disruption to economic, scientific, political and ethical balances would be considerable and likely to redistribute all activities of social life if the emergence of General AI were coupled with developments in robotics, biotechnology or neurotechnology.

1- The Open RAN approach proposes dividing the radio access network (RAN) into several independent technological building blocks, allowing operators to choose suppliers for each block based on their specific needs.

Summary
Field 03 – Technology & Innovation

Major trends effort matrix



Reminder of the assumptions for disruptions by 2040

1. An industrial-scale quantum computing offering is available.
2. The widespread deployment of 6G networks and the generalisation of Open RAN logic are profoundly transforming connectivity and telecommunications networks.
3. Agentic AI is revolutionising a considerable number of websites, software programmes and digital tools beyond the professional world.
4. The first general AI is created.

04 Field

Sustainable digital

Major trends and disruptive hypotheses

Major trends

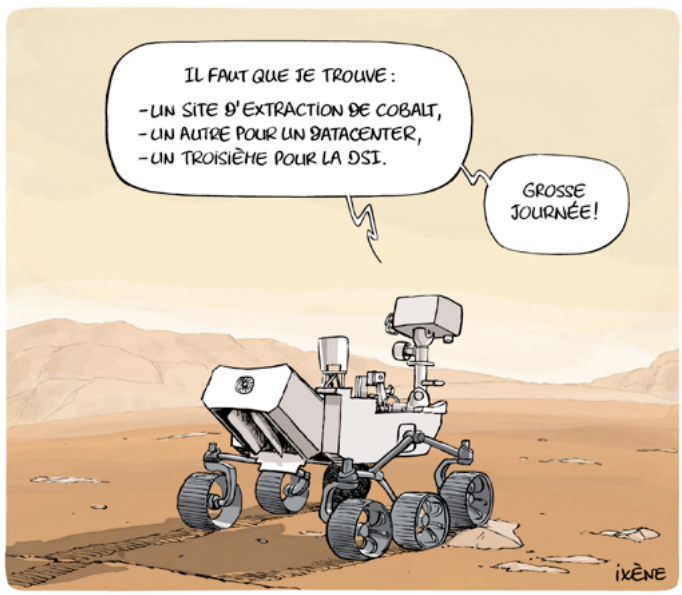
Trend 1. Raw material requirements for digital equipment and infrastructure are growing

Digital technology, too often perceived as "intangible", is primarily based on a foundation of rare, strategic and non-substitutable metals, whose almost exclusive capture by its value chains reveals a systemic dependence. Gallium, germanium, rare earths, indium, tantalum and neodymium are all elements that are often non-recyclable, yet indispensable to current technological performance. Despite their presence in minute quantities in equipment (screens, batteries, motherboards, etc.), their use is so specific that digital technology absorbs up to 95% of global demand for some of them (gallium, germanium).

The extraction and refining of these resources generate major environmental and social externalities, particularly in areas of high political or climatic instability. In Myanmar, rare earth mines contribute to "widespread plundering of natural resources" (Global Witness), in a context of recurrent droughts and poor governance.

The production of these metals relies on co-products or by-products, without a dedicated supply chain, making their availability unstable and unpredictable. Refining is geographically concentrated in China, which accounts for more than 90% of global processing for several of these resources, exposing supply chains to increasing risks of disruption, trade restrictions or strategic reterritorialisation (Global Critical Minerals Outlook 2024). The geographical polarisation of the processing chains for these materials only reinforces their uneven topographical distribution, forcing us to remember that 98% of the rare earths consumed by the European Union came from China in 2024.

> ***Recycling, often presented as a solution, is not yet a viable option.*** *Recycling rates are less than 1% due to the poor quality and complex mix of materials in the terminals. Some electronic waste is exported to open dumps, such as Agbogbloshie in Ghana, where the components are burned in the open air, with major health and environmental consequences. This reality calls into question the sector's ability to integrate a circular approach and highlights the urgent need for structural change.*



By 2040,

resilient control of raw materials could become one of the main criteria for managing the digital function. Indeed, the volumes required in fifteen years' time to meet digital demand could increase tenfold (Annales des Mines). The partial relocation of production, the diversification of sources, the integration of alternative materials and the establishment of cutting-edge recycling channels could become a condition for access to critical digital services. Digital technology could no longer be considered outside of its dependence on physical resources, whose scarcity and conflictual nature would be structuring parameters of a sustainable strategy.

Trend 1.

Trend 2. Extreme weather events are becoming more frequent, with increasing impacts on digital infrastructure and its insurability

Digital value chains are increasingly exposed to the effects of climate hazards, external factors whose frequency and intensity are constantly increasing. For example, several data centres operated by Google and Oracle ceased to function in 2022 due to extreme heat waves, revealing the vulnerability of cooling systems to abnormal temperatures (Wired). In 2024, Hurricane Helen disrupted global production of high-purity quartz when it struck the Spruce Pine mines in North Carolina, illustrating the digital world's dependence on localised resources that are sensitive to climate events.

As the climate system becomes increasingly unstable both globally and locally, risks are diversifying and overlapping: prolonged heat waves, intense droughts, fires, floods, storms, and coastal flooding. Each of these hazards directly or indirectly affects digital infrastructure, whether it be data centres, telecommunications networks, supply chains or industrial sites involved in component production (International Energy Agency). The phenomenon of clay shrinkage and swelling, for example, threatens the stability of the foundations of certain data centres, while forest fires can compromise the power supply or local connectivity, with consequences for service continuity and data security. These climate risks are not limited to physical infrastructure. They also threaten upstream raw material production and associated supply chains (Bloomberg).

Climate change is becoming a factor in economic volatility, heralding more frequent price shocks and supply disruptions that are more difficult to anticipate (France Stratégie). For the digital sector, the consequences are direct and concern both the unavailability of critical components and the slowdown in industrial cycles, as well as increased operating costs. Furthermore, as risks multiply, increasing pressure is being placed on insurance models. Some insurers are beginning to exclude infrastructure located in areas with high climate exposure from their coverage. This development could ultimately render certain digital assets uninsurable, calling into question their economic viability and attractiveness to investors (France Assureurs).

By 2040,

digital climate resilience could become one of organisations' strategic priorities, going beyond simple compliance requirements. Operational requirements could depend on the ability to anticipate risks, adapt technical architectures, diversify geographical locations and integrate business continuity measures. The digital function, as a critical infrastructure, should therefore develop its own climate engineering, capable of combining performance, sustainability and robustness. Insurability would no longer be a given, but a variable to be integrated natively into the financial design of digital projects.

Trend 2.

Trend 3. Access to water for industry and digital players is increasingly constrained by water stress and regulations

Water consumption in the digital sector is growing rapidly, while conflicts over water resource use are becoming commonplace and structural. It is not so much physical water resources that are at issue, but rather quality access to this resource and the simultaneous competition between industrial, agricultural and urban uses. Political decisions on the allocation of this resource are no longer a matter for distant projections. This is evidenced by the 15% reduction imposed by the Taiwanese government on chip manufacturers' water consumption during the severe drought that hit the country in 2021. The consequences for the entire digital value chain were considerable, given that the island produces more than 60% of semiconductors and nearly 90% of the most sophisticated chips. This trajectory therefore places digital technology at the heart of conflicts over land use, with 40% of semiconductor factories expected to be located in areas of high water stress by 2040 (The Diplomat).

Water constraints are leading to a reconfiguration of the models used for the implementation, design and operation of digital infrastructure. Passive cooling, waste heat recovery[1], equipment sharing and algorithmic flow optimisation are increasingly being considered as ways of reducing water dependency. However, these solutions remain marginal at this stage, often costly or complex to deploy on a large scale. In this context, water should no longer be considered as a simple technical resource, but as a strategic variable to be integrated into investment trajectories, digital urbanisation policies and operational resilience criteria.

> *In the digital value chain, water meets at least three main needs. F**irstly, water is used for the extraction and processing of raw materials** needed for infrastructure and material components (semiconductors, processors, etc.), as well as for production and assembly phases.*
> ***Secondly, water plays an essential role in cooling data centres, which consume large volumes of water**. The three main global operators (Meta, Google and Microsoft) alone will consume more than 2.2 billion cubic metres of water by 2022, which is almost double the current withdrawals of a country such as Denmark. Furthermore, **the rise of generative AI technologies, supported in particular by large language models (LLMs), could increase this annual consumption to 660 billion litres of water** (Corell University).*
> ***Thirdly, water is also used indirectly in the production of energy (hydropower, thermal and nuclear) that will be used to power the computing infrastructure and equipment necessary for these uses.***

1- Waste heat is excess heat generated by industrial processes or energy production. Commonly discarded without being used, it represents a significant economic and environmental opportunity.

By 2040,

the water sustainability of digital technology could become an indicator of maturity for organisations. The ability to anticipate local tensions, adapt technical architectures and negotiate access to resources within an evolving regulatory framework may no longer be just an environmental commitment, but a requirement for continuity. As hydrological regimes are expected to become more unstable, digital infrastructure could become more vulnerable to temporary or long-term service interruptions and local protests. Depending on the direct water requirements of organisations' digital activities, water could then become one of the key performance decision criteria.

Trend 3.

Trend 4. The digital sector is contributing increasingly to global energy consumption and GHG emissions

The energy footprint of digital technology is increasing and seems to be on a trajectory that is both faster and more difficult to reverse. Indeed, over the last ten years, energy consumption in the sector has more than doubled in France (ADEME). Furthermore, by 2024, the digital sector will account for nearly 5% of the national carbon footprint and nearly 3.5% of global greenhouse gas emissions. Without even mentioning the long-term orders of magnitude associated with the footprints of satellite constellations, video games and the metaverse (Bon Pote), the current proliferation of terminals (50% of France's footprint) and data centres (46%) already largely reflects the intensification of usage, the growth in data volumes and the rise of computing infrastructure.

The rise of generative functions in artificial intelligence technologies is accentuating this dynamic and marks a turning point in the energy trajectories of digital technology. Large language models (LLMs), due to their algorithmic complexity and computational requirements, consume on average 30 times more energy for text generation and 180 times more for image generation than an interaction on a conventional search engine (Sciences et Avenir). This consumption is not limited to user queries: each training or update phase requires considerable amounts of energy, often from carbon-based sources. For example, the training phase for ChatGPT-3 is estimated to have required 1.29 GWh, equivalent to the annual electricity consumption of 600 French households (Futuribles). This energy dynamic, coupled with exponential growth in usage, makes any stabilisation of the sector's energy expenditure highly unlikely in the short term. Even the emergence of more specialised and frugal models, such as Small Language Models (SLMs), is not enough to reverse the trend. In the absence of political regulation of usage or rigorous targeting of AI activities with high added value for all, process optimisation and the democratisation of services through AI will tend to significantly increase energy consumption rather than contain it.

Faced with this growing pressure, digital giants may be tempted to secure their energy supply by appropriating very limited resources. Without even mentioning exclusive nuclear energy supply agreements, Amazon, Meta, Google and Microsoft have already acquired nearly 29% of new global wind and solar contracts in 2020 (Bloomberg). This trend suggests potential conflicts of use with other strategic sectors, which could suffer, without prior preparation, from service disruptions due to energy supply cuts.

By 2040,

the energy sustainability of digital technology could become a strategic management criterion for organisations, given that data centre energy consumption could triple by 2030 and account for up to 6% of French consumption by 2050 if no countermeasures are taken (ADEME). On a global scale, the International Energy Agency (IEA) estimates that without major changes, the share of electricity production absorbed by data centres could reach 14% by 2040. The ability to measure, anticipate and reduce the energy footprint of digital services would then no longer be a matter of reporting and compliance, but a requirement for growth, competitiveness and resilience. In addition to increased efforts to improve energy efficiency and robustness, the systematic integration of eco-design standards, energy-efficient architectures, optimised language models and regulatory mechanisms adapted to the reality of infrastructure could represent the new normal for Digital Responsibility.

Trend 4.

Trend 5. European regulations governing digital activities in order to reduce their environmental impact are gaining significant momentum compared to other less proactive powers

The European Union is gradually establishing itself as one of the main regulatory bodies for responsible digital development. Through a comprehensive series of texts (from the WEEE[1] and Baueries[2] directives, the Critical Raw Materials, Net Zero Industry and ESPR[3] regulations, to the upcoming Circular Economy Act and Advanced Materials Act), the EU is designing a regulatory framework that no longer merely encourages, but compels. The descriptive passport detailing the composition of digital products, recyclability requirements, eco-design criteria and component traceability requirements are part of a capacity-based regulatory approach aimed at reducing the sector's material and energy footprint.

1- The European Union has defined the conditions for placing EEE on the market and the framework for the management of waste electrical and electronic equipment (WEEE). The 2012 WEEE Directive sets out obligations for the collection, treatment and recycling of electronic waste and makes manufacturers responsible for the end of life of their products.
2- The 2006 Battery Directive aims to limit the environmental impact of batteries, particularly that of the harmful substances they contain, such as mercury, cadmium and lead.
3- The Ecodesign for Sustainable Products Regulation is a European regulation promoting the eco-design of sustainable products. Adopted in June 2024, it establishes a digital product passport system that will provide access to key information on the entire product life cycle, including composition, materials used, repair possibilities and product recycling options.

> ***The European dynamic is not limited to production or distribution: it extends to uses, infrastructure and economic models****. Impact measurement obligations, restrictions on terminals, calls for equipment sharing or software sobriety are redefining the room for manoeuvre available to digital departments. Digital technology is becoming a separate regulatory object, subject to the same requirements as other industrial sectors. Despite strong opposition to the latest sustainability reporting project (CSRD directive), this standardisation process could ultimately structure the environmental compliance market, with its indicators, certifications and sanctions.*

Globally, there are currently no binding regulations governing the environmental footprint of digital technology. These issues are, of course, discussed within the G20 and the UN (UNEP). **However, the United States does not have any federal legislation specific to the digital sector**. Initiatives are mainly driven by voluntary companies in the sector or certain federal states, such as California (Deloitte) or New York State (NY State). A bill entitled "Artificial Intelligence Environmental Impacts Act of 2024" aimed at assessing the environmental impacts of AI has been introduced in the Senate but has not yet been passed (GovTrack). **China, on the other hand, has incorporated the reduction of the digital carbon footprint into its sovereignty plans**, announcing its intention to achieve carbon neutrality by 2060 (Le Monde). In particular, the Chinese authorities are imposing energy efficiency standards for data centres and encouraging the use of renewable energies in the digital sector.

By 2040,

the ability of organisations to integrate environmental regulations into their digital strategy could become a differentiating factor. In a world of ecological constraints that are likely to become more stringent, French and European digital technology seems unlikely to develop effectively and profitably without a demanding regulatory framework. By structuring this framework, France[1] and Europe would benefit not only from managing risks, but also from redefining the conditions for sustainable technological progress. Provided that organisations realise the benefits of "IT for Green", Digital Responsibility could then become a powerful lever for competitiveness, resilience and legitimacy.

Trend 5.

1- It should be noted that in France, specific laws aim to regulate the digital footprint. This is the case with the Law on Reducing the Environmental Footprint of Digital Technology (2021), which requires local authorities with more than 50,000 inhabitants to define a sustainable digital strategy. The same spirit is at work with regard to the observatory of the environmental footprint of digital technology. The Anti-Waste and Circular Economy Act (AGEC, 2020) also encourages the repair of digital equipment and combats planned obsolescence. The government has also created a sustainable digital label (LNR), which aims to support and promote organisations that are committed to reducing the impact of digital technology.

Trend 6. Practices aimed at reducing the energy and resource consumption of digital technology are developing

Faced with the growing effects of climate change, regulatory pressure and civil society demands, organisations seem to be starting to transform their digital practices. Although usage accounts for only 20% of the environmental impact of digital technology, 85% of French people consider it to be a cause for concern (ADEME). Energy efficiency, long confined to marginal initiatives, is increasingly becoming part of organisations' overall strategies. Digital departments are now incorporating environmental footprint reduction targets into their roadmaps, with associated performance indicators.

IT architectures are increasingly being redesigned to promote pooling, decentralisation and load optimisation, which is also made possible by edge computing. Digital software and services are also increasingly being developed, from the outset, using shared eco-design standards to reduce their carbon footprint and hosting and maintenance costs, while extending their lifespan (ARCEP - ARCOM). The use of data centres powered by renewable energy and innovative cooling solutions (free cooling, use of outside air or data centre immersion), the implementation of end-of-life policies for equipment, and the extension of hardware renewal cycles are becoming standard practice. These developments are part of a systemic responsibility approach, where each technological choice is evaluated in terms of its ecological impact. This dynamic is also driven by cultural and organisational change. Digital teams are increasingly aware of environmental issues, and digital sobriety skills are becoming differentiating criteria for recruitment and training.

By 2040,

energy-saving practices could converge towards a model of digital frugality, where value creation would no longer depend on increasing technological intensity, but on the careful and efficient management of the resources used. Organisations capable of implementing this frugality without sacrificing agility or competitiveness could be better equipped to respond to energy constraints, beyond the regulatory factor alone. Digital technology would no longer be solely a vector of efficiency, but would become a field of environmental excellence.

Trend 6.

Trend 7. The potential of digital technology to optimise energy consumption is increasingly valued

As tensions over energy resources intensify, digital technology is fuelling the ambitions of those who would like to make it a major lever for energy efficiency across all sectors of activity. Without succumbing to techno-utopian solutions, digital technology is increasingly being used as a tool for orchestrating, managing and optimising energy flows at the level of organisations, territories and infrastructure. This revaluation as a vector of sobriety is transforming the strategic priorities of the digital function, which is set to play a central role in the energy transition.

Information systems now incorporate data sensors and advanced functions for monitoring, predicting and optimising energy consumption and electrical flows (heating, lighting, cooling, etc.). Distribution networks, smart grids, platforms and energy management applications promote a systemic approach to energy performance. The Internet of Things (IoT), combined with artificial intelligence, also enables precise management of the resources required for buildings, supply chains and mobility networks. Digital twins, by simulating energy behaviour, also offer the possibility of real-time decision-making and waste reduction.

By 2040,

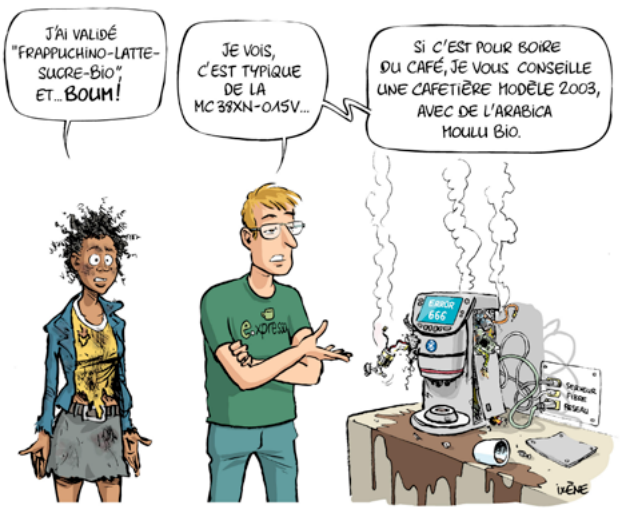
in a context of energy scarcity, organisations capable of leveraging the energy-digital synergy could have a decisive competitive advantage. Harnessing the diversity of solutions offered by the digital environment could be accompanied by a shift in business models. Under the weight of energy prices, organisations would invest in solutions capable of generating the most measurable energy savings, and return on investment indicators would systematically incorporate the environmental dimensions of "green capitalism". Digital technology would then not only be at the heart of sustainability strategies, but would also be a driving force behind resilience and competitiveness policies, working closely with real estate, industrial and CSR departments to design integrated guidelines. Under these conditions, digital technology could easily meet the challenge of convergence between operational efficiency and responsibility.

Trend 7.

Trend 8. Research and development to access more sustainable electronic materials and optimise digital energy consumption is growing

Against a backdrop of growing geopolitical, regulatory and environmental pressure, R&D programmes are being implemented to reduce the sector's environmental impact and promote the eco-design of digital solutions. Numerous public laboratories, industrial consortia and deep tech start-ups are already converging towards the common goal of designing electronics that are more energy-efficient, more sustainable and less dependent on critical supply chains.

R&D efforts aimed at transforming the physical structures of digital technology focus on at least two strategic areas. On the one hand, they concern the improvement of manufacturing processes, in particular by reducing chip architecture or the firing temperature of electronic components, and the use of advanced 3D printing techniques, which reduce the energy footprint of new-generation chips. Projects focusing on the repairability, modularity and recyclability of electronic equipment aim to extend their lifespan and facilitate their reintegration into circular cycles. **Secondly, development programmes are striving to discover and use alternative materials to rare earths and critical metals on an industrial scale**. Despite currently less competitive performance, research into graphene, organic semiconductors and conductive polymers (L'Usine Nouvelle) is slowly paving the way for electronics that are less extractive, less energy-intensive and biodegradable (Science Advances).



By 2040,

these advances could redefine industrial standards in the digital sector. Organisations capable of developing alternative and innovative technologies or quickly integrating them into their infrastructure would then enjoy a competitive advantage in terms of resilience and social responsibility. Many promising technologies could reach maturity, such as zinc batteries (L'ADN), cold data storage[1] , on DNA (CNRS) or on ceramics (L'ADN). By overcoming issues such as storage capacity, equipment lifespan and manufacturing costs, R&D could then become a strategic pillar of digital sustainability, serving technological progress aligned with planetary boundaries.

Trend 8.

1- "Cold" data is not intended to be consulted regularly

Hypotheses of disruption by 2040

1. The EU requires industry to recycle and reuse almost all electronic components.
Digital players would be forced to radically overhaul their production chains. This could stimulate innovation in more sustainable materials, but would also require major investment from players in the sector.

2. Certain digital infrastructures are no longer insurable.
Faced with increasing climate risks, insurers could refuse to cover certain digital infrastructures deemed too exposed. This would call into question the economic viability of certain projects and force operators to strengthen their resilience to this type of risk.

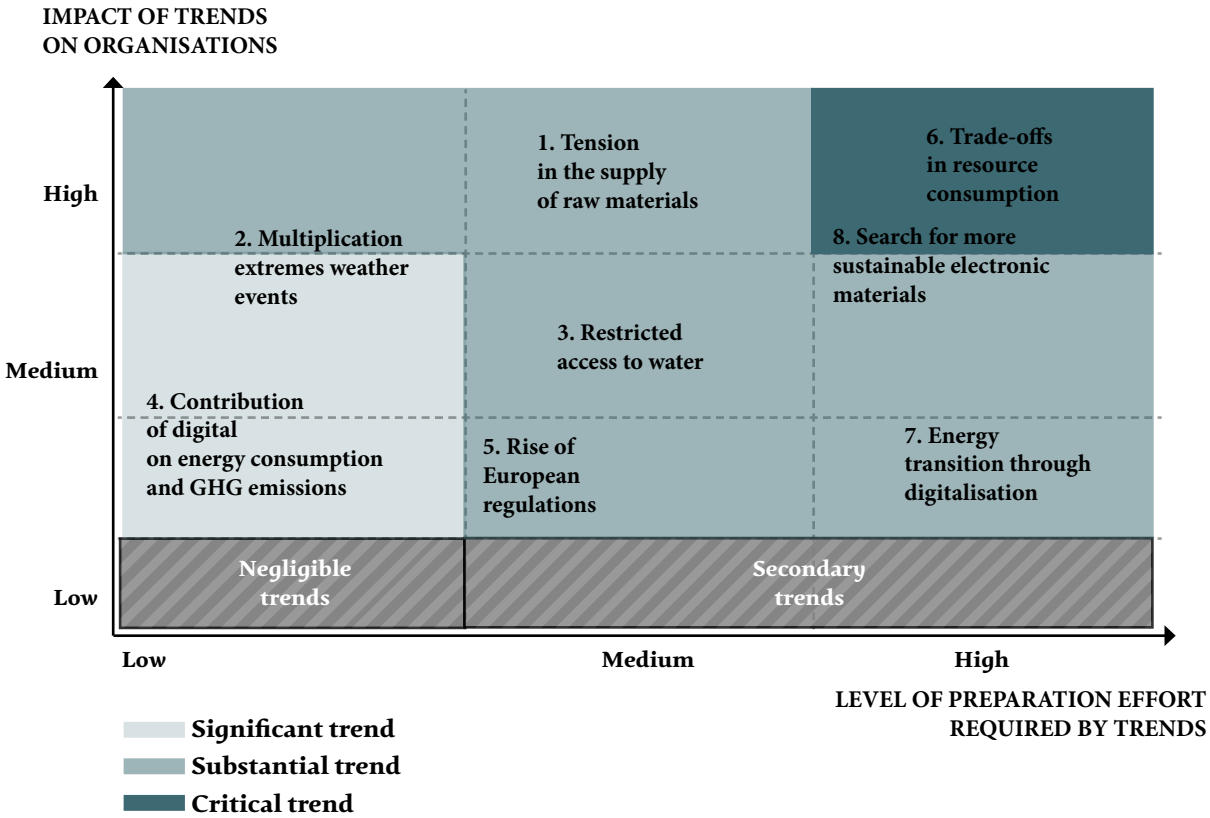
3. Energy is the subject of conflicts of use due to the widespread use of AI.
In a context of growing energy needs, access to certain digital services deemed too energy-intensive or unnecessary would then be restricted in order to limit the impact on the environment and resolve conflicts of use.

4. The digital sector faces constraints on its water supply.
With conflicts over the use of water resources, particularly in areas with a high concentration of data centres, access to water is becoming a source of tension between economic players, including those in the digital sector, but also with civil society.

5. The production of certain raw materials essential to the digital industry has been relocated to France.
France is reviving the exploitation of critical raw materials on its territory, such as certain critical metals, in order to secure its supplies and limit its dependence on other powers such as China.

Summary
Field 04 – Sustainable digital

Major trends effort matrix



Reminder of the assumptions for disruptions by 2040

1. The EU requires the industry to recycle and reuse almost all electronic components
2. Some digital infrastructure is no longer insurable.
3. Energy is subject to conflicts of use due to the widespread use of AI.
4. The digital sector faces constraints on its water supply.
5. The production of certain raw materials essential to the digital industry has been relocated to France.

05 Field

Digital & Society

Major trends and disruptive hypotheses

Major trends

Trend 1. The labour market is facing growth and diversification in skills requirements

As technological transformations accelerate, the labour market is entering a phase of restructuring. A driving force in employment dynamics, the digital sector is also suffering from the shortcomings of this market, caught between steadily increasing recruitment needs and difficulty in attracting sufficient talent. Indeed, skills requirements are constantly growing and diversifying, driven by the combined effects of artificial intelligence, cybersecurity and the ecological transition. This evolution does not only affect technical professions, but all functions, from management to customer relations and support functions.

The digital sector is experiencing sustained growth in the number of jobs, but is struggling to fill the positions available, even though it was already ranked among the sectors under the most pressure by France Travail and DARES. In 2024, the sector will have nearly one million employees, an increase of more than 50% in fifteen years. However, 80,000 positions remain vacant (Institut Montaigne), and up to 85% of recruitments are considered difficult (France Travail). The most sought-after skills (cybersecurity, finops, cloud architectures, artificial intelligence) are evolving very rapidly, requiring continuous updating of expertise.

> ***The tensions are both quantitative and qualitative, divided between growing needs and the logic of re-internalising skills on the one hand, and increased demands for specialisation, adaptability and continuing education on the other***. *Furthermore, this dynamic is taking place in a contrasting demographic context. The ageing of the working population, mass retirements and the expected decline in the working-age population from 2040 onwards will accelerate these imbalances. More than half of the working population will then be over 50, raising questions about skills, technical debt and retraining. New challenges may also emerge around cohabitation and intergenerational transmission, as more than four generations will be called upon to work together simultaneously. Organisations will need to rethink their HR strategies in order to attract, train and retain talent in an environment of scarcity, marked by increased regional inequalities (Graduate School of Digital Technology).*

By 2040,

the genuine organisational resilience of businesses and administrations could become a differentiating factor in attractiveness, loyalty and managerial innovation. This resilience would largely depend on organisations' ability to anticipate skills needs and translate them into increasingly flexible job descriptions in order to structure agile and personalised training pathways (from internships or work-study programmes to retraining through reskilling, including internal mobility and upskilling). Organisations would then be able to optimise the diversity and hybridity of the skills needed to meet digital needs, ranging from ethics and humanities to IT and fundamental research in biophysics, change management and soft skills, strategy and governance, bot-to-bot design and customer experience, and risk management, data intelligence and engineering. Given the social and therefore political importance attached to digital technology, technology leaders could gradually take on the role of orchestrators of "human development" by strengthening the conditions for cooperation between educational institutions, centres of research excellence and the territorial network of organisations.

Trend 1.

Trend 2. GAI is becoming established in professional use, often outside organisational frameworks

Generative artificial intelligence (GAI) has established itself in just a few years as an essential tool in professional environments. Its adoption, often widespread and spontaneous, is disrupting work practices, organisational models and governance balances. One-third of organisations with 10 or more employees are already using AI in 2024, with adoption rates reaching 50% in industry and 40% in commerce and finance (France Travail). Another third are conducting experiments to explore its potential uses. While more than 7 out of 10 organisations believe that AI improves the skills and performance of their employees, the cost of solutions and the lack of internal expertise are still hindering widespread use.

> ***The professional uses of IAG are mainly structured around three dynamics. Firstly, the partial automation*** *of repetitive or time-consuming tasks (writing, summarising, translating, developing, administering), which improves productivity but can also lead to technological and intellectual decline, particularly among recent graduates.* ***Secondly, a reconfiguration of professions****, where AI becomes a cognitive assistant, increasing analytical, creative and decision-making capabilities.* ***Thirdly, the emergence of new roles and areas of expertise*** *(prompt engineers, model curators, algorithm auditors), which seem to be gradually redefining the skills required in organisations.*

The rapid expansion of this technology, which is currently open to all, is accompanied by significant grey areas. In many organisations, IAG is used daily by employees, sometimes outside any official framework, via personal accounts or unapproved tools. The lack of formal oversight by the digital department, the lack of user training, and the inadequacy of internal oversight policies expose organisations to multiple risks such as sensitive data leaks, algorithmic bias, and regulatory non-compliance. The adoption of the AI Act at European level should make it possible to establish a more robust framework, but its implementation remains gradual, and organisations must anticipate future requirements now.

The impact on employment is mixed. While AI can help alleviate certain labour shortages and improve the quality of certain jobs, it could also lead to job losses, including skilled jobs. In France, up to 800,000 jobs could be at risk, according to some estimates, while 1.4 million could be "augmented" by AI (Roland Berger). At this stage, pay scales could be reconfigured according to the complementarity and replaceability of jobs by AI-generated functions. This polarisation of the labour market requires increased vigilance with regard to career paths, continuing training and transition management.

By 2040,

IAG could become a cognitive infrastructure as essential as traditional information systems. Training in its appropriate, targeted use in line with organisational policies should have reached a level of maturity. Organisations capable of supervising its use, controlling its risks and leveraging its contributions to their activities could have a real advantage. The implementation of programmes aimed at maintaining employees' skills complementary to AI technologies could be a strategic lever for organisations. These skills – the ability to seek out and recognise good ideas, organise and prioritise them, turn them into desirable objectives, assess and choose the means to achieve them, evaluate their potential impact, and engage in logical and ethical reasoning – could enhance human added value and increase synergies tenfold in an increasingly technology-driven professional environment.

Trend 2.

Trend 3. The physical and mental health of workers is gradually deteriorating

The world of work is undergoing a phase of intensifying health risks, marked by a gradual deterioration in the physical and mental health of the working population. This trend affects all sectors, but is particularly evident in digital professions, where the pace of change, cognitive demands and working conditions create specific vulnerabilities

> ***Demographic dynamics, working conditions and the phenomenon of "mental fatigue" are all factors that support this trend**. Firstly, the ageing of the working population is accompanied by an increase in chronic conditions, whether work-related or not. In fact, nearly a quarter of 50-64 year olds, or 5% of the total French working population, suffer from a long-term illness (ALD). Secondly, current working conditions are conducive to an increase in musculoskeletal disorders (MSDs) due to sedentary lifestyles, prolonged sitting and lack of physical activity. Thirdly, mental health is increasingly undermined by stress, cognitive overload and professional uncertainty. In the space of a few years, the proportion of employees affected by mental health issues has doubled, reaching 10% of women and 2% of men, while one in four French employees report poor mental health, with young people and full-time teleworkers being the most affected (Ipsos Qualisocial Barometer 2025).*

In the digital sector, health risks seem to be amplified by the very nature of the activities involved. The rapid pace of technological and managerial change requires constant adaptation, generating anxiety about skills becoming obsolete, particularly among highly specialised profiles. The spread of generative artificial intelligence (GAI) is exacerbating this pressure by changing professional benchmarks and raising concerns about the sustainability of jobs. Furthermore, teleworking, although appreciated for its flexibility, can promote isolation, a loss of collective benchmarks and an intensification of invisible work.

By 2040,

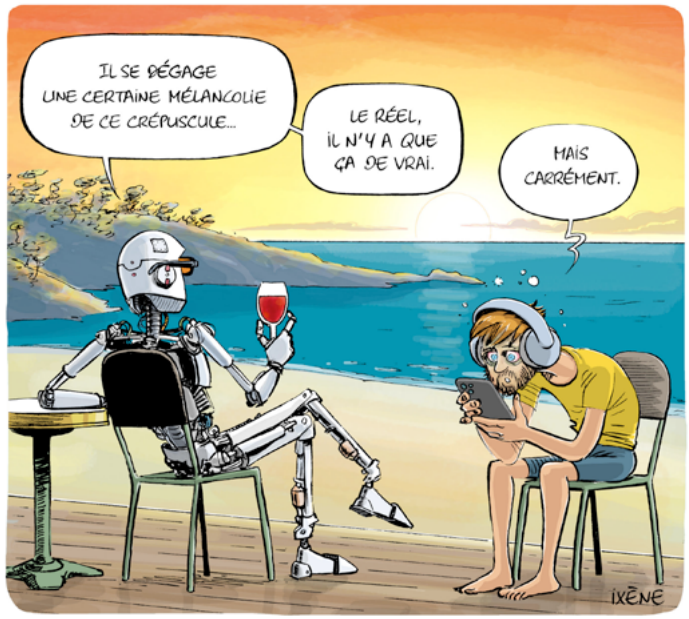
the health of workers could become a key factor in organisational resilience and long-term competitiveness policies. Organisations capable of designing working environments, rhythms and tools that promote the "integral development" of their employees at all stages of their working lives should significantly enhance their attractiveness and foster stable, high-quality engagement. A re-evaluation of digital practices could involve identifying activities that require significant exposure to large amounts of information, systematic presentation materials and screens in general. The implementation, from the start of an employee's career, of personalized and scalable support programs for the regular maintenance of their physical, moral, and mental strengths could become a definite asset in anticipating the increase in the average retirement age.

Trend 3.

Trend 4. Digital technology is now at the heart of health issues

The widespread use of digital technology in all areas of daily life is transforming public health issues, both as a lever for prevention and support and as a potential source of physical, mental and social risks. Health can no longer be considered outside the influence, however small, of digital technology, and digital technology can no longer be deployed without consideration for its health impacts. The dual dynamics of risk and opportunity brought about by digital technology require organisations, and in particular digital functions, to exercise greater vigilance and take on greater responsibility.

> ***The harmful effects of excessive or inappropriate use of digital technology are now well documented.*** *Among young people in particular, excessive screen time is correlated with a decrease in sleep, physical activity and sociability. Teenagers (aged 12-19) have an average of three personal screens (mobile phone, television, computer, etc.) and spend nearly 20 hours per week on the internet. Children aged 5-12, meanwhile, spend nearly 5 hours per week online (IPSOS). Musculoskeletal and ophthalmic disorders, concentration problems, and feelings of isolation and anxiety are on the rise. Certain extreme cases of suicides "encouraged" by AI, after prolonged interactions with conversational agents, raise unprecedented ethical questions about the responsibility of designers and platforms (Futuribles). Mental health, already weakened by professional pressures, the fragmentation of the family unit and social uncertainties, can be further aggravated by unregulated digital use.*



In another respect, digital technology is at the heart of healthcare issues as a source of powerful solutions. Indeed, telehealth tools and medical monitoring platforms, connected devices for seniors, disabled people or patients with chronic illnesses, and AI diagnostic aids are helping to improve prevention through personalised monitoring and enhanced coordination of care pathways. In 2024, 90% of French people say they have already used a digital health service, and a majority believe that these tools improve the quality of medical monitoring (DNS). The potential of social AI or companion AI is also highlighted for certain well-targeted social interactions (isolated individuals, complex therapies). On the other hand, nearly 8 out of 10 French people say they are concerned about the commercial uses that could be made of their health data.

By 2040,

the ability to combine technological innovation and health sustainability could become a criterion of legitimacy for organisations, going beyond well-being at work. The promotion of digital practices could involve specifically targeting activities that involve intensive use of screens. The aim would be to diversify the senses and faculties used (sight, hearing, speech, touch) in order to reduce exposure time while improving quality. The digital function would have a strategic role to play in this innovative transformation, contributing to risk prevention, raising employee awareness and guiding them towards more sustainable use. Faced with growing fears of a "diminished human being" due to technology, organisations capable of designing regenerative digital technology, based on emotional intelligence and geared towards widespread "care management", would strengthen their attractiveness, resilience and social contribution.

Trend 4.

Trend 5. French society enters the post-truth era

The proliferation of information sources, the virality of content, the algorithmic optimisation of attention spans and the rise of generative technologies have profoundly altered the cognitive benchmarks of French society. The realism of principles, logical demonstration and its universal scope, and confirmation by facts, once the foundation of the "public spirit", are giving way in part to fickle opinions, herd mentality and personalised narratives.

This trend is not simply a marginal and involuntary shift brought about by a change in the technological context. It constitutes a civilisational transformation, partly voluntary, of our relationship to reality, reason, knowledge, trust, legitimacy, authority – and therefore to all forms of truth. With the post-truth era, we are entering post-modernity, that is to say, a post-Enlightenment era in which the rationalism designed for the democratic ideal is faltering. Recent surveys reveal a growing vulnerability to disinformation. While 76% of French people believe they are able to distinguish between true and false information, two-thirds of them actually believe at least one piece of false information (IPSOS).

The blurring of the lines between truth and falsehood is accentuated by the widespread use of generative artificial intelligence tools capable of producing, with disturbing realism, low-cost falsified content, deep fakes, manipulated texts, and synthetic voices. The use of these tools as search engines or cognitive assistants, without verification of sources, reduces the capacity for critical reflection and promotes information lock-in (the ability to diversify sources and points of view). In this context, the internet and social media become ambiguous, serving both as spaces for expression and as channels for polarisation and fragmentation of public debate. Platforms are increasingly being called upon to take responsibility, but regulatory mechanisms are struggling to keep pace with innovation. Digital identity security measures, trust labels and verification bodies are developing, but are still insufficiently or poorly integrated into everyday use.

By 2040,

the ability to navigate a saturated, unstable and sometimes manipulated information environment will become a strategic skill. Indeed, the consequences of this trend are likely to extend far beyond the media sphere and affect social cohesion, organisational governance and individual and collective decision-making. Obtaining and retaining high-quality data will be more important than ever, given that the circulation of unverified information could undermine internal trust, damage external reputation and compromise data security. Organisations capable of guaranteeing the reliability, traceability and plurality of the data they produce and consume should considerably strengthen their legitimacy and resilience. Digital functions would have a key role to play in anticipating these risks by strengthening information monitoring and verification systems and awareness-raising initiatives. The ability to discern, make conceptual distinctions, prioritise information, apply nuance, exercise caution and humility, and other interpersonal skills could then become real assets for employees.

Trend 5.

Trend 6. Cyber risks are intensifying and diversifying

The ubiquity of digital technology in professional, personal and institutional spheres is accompanied by a continuous expansion of cyber threats. The question is no longer "who will be the next target?", but "when will I be attacked?". Attacks are no longer exceptional events and are becoming an almost routine part of the digital landscape, affecting all sectors, all sizes of organisations and all user profiles. This diversification of risks, through the cross-multiplication of attack surfaces and the forces of attackers via AI, is transforming cybersecurity strategies based on anticipation, resilience and cooperation.

> ***The cyber threat in France has been steadily increasing since 2020, as evidenced by the 15% rise in the number of incidents handled by ANSSI in 2024****. The increase in distributed denial-of-service attacks (DDoS attacks doubled in 2024 compared to 2020) reflects the sophistication of strategies to destabilise critical systems, while the increase in attacks targeting operational assets, particularly industrial systems, will have a reinforced capacity to cause damage. In France, malware attacks will be widespread in 2024, with 144 compromises recorded, 12% of which will target higher education establishments and 12% strategic companies. Microbusinesses, SMEs and mid-cap companies remain the main targets, accounting for the majority of victims. For these organisations, the consequences can be critical: prolonged service unavailability, damage to reputation, and a more than 50% risk of bankruptcy in the months following the attack (BreizhCyber). Large organisations are not spared, but generally have more structured response capabilities. Individuals are increasingly exposed to various forms of cyber malice, scams, phishing, and identity theft, often amplified by media coverage of false claims of data exfiltration. ANSSI emphasises that these threats contribute to growing mistrust of digital technology, particularly in sensitive sectors such as social services, health and employment.*

Faced with this multifaceted threat, protection measures are evolving and cybersecurity is becoming less and less confined to a technical support function. It is becoming a shared responsibility at the highest levels of the hierarchy, integrated at all levels and across all departments of the organisation within a comprehensive digital security governance framework. Depending on organisational models and the reporting structure of the CISO function, the digital function combines preventive approaches (definition of digital security policy and day-to-day application) and reactive approaches (continuity plans, crisis units, partnerships with the relevant authorities) to a greater or lesser extent.

By 2040,

Cyber risks could become one of the main factors contributing to the vulnerability of organisations and individuals. Developing and maintaining a culture of cybersecurity, on whatever scale, could become a key skill. Trust, training and innovation around the human factor could be essential means of strengthening resilience. In this paradigm, cybersecurity would no longer be perceived as a cost but as a strategic asset that is crucial to the continuity of service and the sustainability of the activities of both individuals and organisations.

Trend 6.

Trend 7. Workers' expectations are becoming increasingly diverse

The relationship to work is undergoing a transformation driven by more assertive individual aspirations and renewed collective demands. French and European women currently seem to be focusing on the concepts of meaning in work, recognition and trust, flexibility and genuine consideration for employee well-being (Institut Montaigne). Surveys conducted in recent years reveal growing ambivalence: while nearly 80% of employees say they are generally satisfied with their work, a majority still express persistent frustrations. Remuneration, considered insufficient by nearly half of the workforce, remains a major point of tension, as does the increase in workload. Aspirations also relate to working conditions, the quality of interpersonal relationships with colleagues or direct management, work-life balance, and access to remote working (IFOP). In the digital sector, these demands are particularly exacerbated by project-based working methods, occasionally very high workloads and unstable teams, which generate a particular feeling of lack of recognition.

Employees' relationship with their organisations has also deteriorated over the past decade. Only 20% say they are "very" proud to belong to their organisation, half as many as twenty years ago. Half believe that their organisation does not take sufficient account of their needs and the real constraints of their jobs. Organisations must also contend with more fragmented career paths and contrasting generational differences that go beyond purely economic considerations and touch on fundamental values such as commitment, loyalty, authority and autonomy.

By 2040,

team cohesion and recognition of individual contributions could play an increasingly important role in the sustainable performance of organisations. In a context of continuous transformation of working environments, the role of direct manager or hierarchical figure combining operational leadership and active listening could be increasingly sought after by workers, particularly in digital jobs. The organisational and cultural reinforcement of this qualitative trend could foster motivation, commitment, a sense of duty and a job well done among employees. Digital tools (collaborative platforms, shared dashboards, AI assistance) could support this transformation in a humane and sustainable manner, facilitating the coordination of efforts, the monitoring of skills, the clarity of collective objectives and the transparency of decision-making processes. Organisations capable of fostering a renewed form of engagement at work would then strengthen their attractiveness and resilience.

Trend 7.

Trend 8. New working and management methods are developing to meet employees' new expectations

Faced with the diversification of employees' work patterns, organisations are questioning their working practices and management models. To a certain extent, teleworking, catalysed by the health crisis, has become established practice (INSEE). A quarter of employees will be teleworking regularly in 2024, with an average of two to three days per week. However, this pace, considered optimal by a majority of employees and managers, conflicts with the "return to the office" policies[1] of many organisations (International Business Times). This way of working nevertheless gives rise to debate and frustration. Working hours are perceived as longer, the practice varies according to socio-professional categories (65% of managers, 10% of employees) and it increases the risks of isolation and fragmentation of collective sentiment. In the digital sector, where two-thirds of employees regularly telework (DARES), the issue of team cohesion is becoming central, as are the conditions of teleworking (at home, at a client's premises, in a co-working space), which influence the employee experience.

> ***Beyond teleworking, new ways of organising working time are emerging**. The four-day week, which has been trialled by several organisations, appeals to nearly 70% of French people. By 2025, more than 10,000 employees will already be working this way (IFOP). This reorganisation, although still marginal, reflects a desire to reconcile performance and quality of life, while responding to the aspirations of younger generations. It challenges productivity models, collaboration rhythms and coordination tools.*

By 2040,

maintaining a balance between employers and employees could become a subject of debate within organisations. The optimisation of processes made possible by AI is already having a considerable impact on employees in offshore digital entities. These upheavals could very quickly affect the social and organisational model of teams based in France and Europe. From the employers' point of view, two models of digital team engagement could emerge: on the one hand, an increased quest for productivity based on the orchestration of AI and the personal investment of on-site employees; on the other hand, the search for a dynamic of collective emulation within teams, mobilised to face the prevailing uncertainty. Organisations capable of offering a synthesis of these two models, combining the social purpose of work with agile realism in terms of resources, should be able to strengthen their attractiveness and their ability to retain the best talent in the long term. In any case, the renewal of organizational culture and the value proposition associated with work should be at the heart of future employer-employee relations.

Trend 8.

1- Post-COVID organisational policies, also known as RTO, or "Return To Office"

Trend 9. Digital divides persist and become more complex

As digital technology becomes essential for accessing services, information and employment, the ability to use these tools is becoming crucial for both personal and professional needs. However, inequalities in the use and mastery of digital tools are not particularly diminishing; rather, they are transforming and tending to increase. Digital illiteracy, long marginalised, affects up to two-thirds of people over the age of 75 (Vie publique). In addition, a quarter of French people feel that they do not have sufficient mastery of digital tools to be able to use them fully (Crédoc). Beyond access to digital technologies, it is now the ability to understand and appropriate them that lies at the heart of the new divides. These inequalities may be invisible, but they are nonetheless fundamental to the social and professional inclusion of the most disadvantaged, the most vulnerable and the least educated.

> ***There are many causes for the increasing complexity of digital divides**. Firstly, the rapid pace of technological change and diffusion is creating a growing gap between the tools available and the skills needed to use them. It should be noted that the widespread use of AI companions could, however, facilitate digital use by making it more fluid and intuitive, even for non-experts. Secondly, the widespread use of online procedures, accelerated by digitisation policies, requires a minimum level of technical proficiency in order to access rights, services or employment. Thirdly, digital practices are diversifying, with increasingly complex interfaces, terminals and interaction logic, which can exclude those who are less familiar with them.*

Public policies are attempting to address these issues through support, mediation and training measures. The "France Numérique Ensemble" plan aims to reach 8 million people who are digitally excluded, train 20,000 support workers, distribute 2 million refurbished computers to the most disadvantaged households, and open 25,000 digital mediation centres. However, these efforts are struggling to keep pace with technological change, and there remains a gap between the implementation of these measures and the public's ability to assimilate them. Numerous committed citizen and community initiatives play an essential role, but remain fragmented and often under-resourced (MEDNUM).

By 2040,

digital divides could shift towards more subtle but equally exclusionary forms: an inability to interact with conversational agents, to understand AI results, or to configure one's digital rights. Inclusion would no longer be just about access to tools, but about the ability to exercise informed digital citizenship. Organisations could integrate this requirement into their strategies for designing, distributing and supporting interfaces, products and services.

Trend 9.

Trend 10. Digital sobriety practices are developing in response to the social, health and environmental impacts of digital technology

Faced with the omnipresence of digital technology in contemporary lifestyles, a collective awareness is emerging around its negative externalities. In response, practices of digital sobriety are gradually spreading throughout society, driven by citizens, organisations and public authorities concerned with making virtuous use of technological tools. This dynamic, still in its infancy, could define a new relationship with digital technology, based on moderation, responsibility and sustainability, as a counterpoint to trends that contribute to the deterioration of mental health, the impoverishment of social relationships and the increase in individual environmental footprints.

> ***In terms of health**, official French recommendations call for limiting children's exposure to screens, or even banning it before the age of three (Commission écran). Debates on regulating digital use in public and family spaces are multiplying, reflecting a desire to preserve social and cognitive balance (ARCEP). The majority of French people believe that digital technology already occupies too important a place in society, and two-thirds consider it dangerous for society. Nearly 40% say they themselves spend too much time on screens, a third believe that digital technology is detrimental to social relationships, and 80% believe it is harmful to children's development. Internationally, certain radical measures illustrate the extent of concerns related to addiction and visual health, such as in Chile, where adolescents' gaming time is limited to three hours per week (Le Monde).*
> ***In environmental terms**, digital uses, although they represent only 20% of the sector's overall impact (ADEME), are increasingly being called into question. Eighty-five per cent of French people consider the environmental impact of digital technology to be a concern, and the majority believe that digital technology occupies an excessive place in society (ADEME). This awareness is also reflected in changes in behaviour. Nearly half of French people now keep their smartphones for at least two years, a significant increase in five years (ARCEP). Usage patterns are being re-evaluated: shopping, socialising and administrative procedures are increasingly being carried out in person, by choice. Organisations, for their part, are beginning to integrate sustainability criteria into their digital policies, through the limitation of video streams, the rationalisation of equipment, the eco-design of services and the systematic awareness-raising of employees.*

By 2040,

digital sobriety could become a key factor in the social acceptability of digital technology. Faced with growing opposition to the technological footprint on everyday life, promoting a strategy of 'digital temperance' could become a real means of social pacification. Digital technology could no longer be thought of solely as an 'unlimited and immaterial resource', but as a means of achieving the common good, to be preserved, regulated and shared with discernment. Organisations capable of reconciling targeted technological performance with moderation of use, in particular by reducing superfluous practices, extending the life of equipment and empowering users, could strengthen their organisational resilience. They would then gain in terms of support, collective commitment, and human productivity.

Trend 10.

Hypotheses of disruption by 2040

1. Advances in AI are leading to a profound reconfiguration of a large number of professions.
The rapid pace of AI progress could have a major impact on many professions, including the most skilled ones. According to the IMF, two-thirds of occupations in developed countries are highly exposed to AI technologies. Of these, one-third could be directly replaced by AI, and one-quarter could be reconfigured to incorporate its contributions (EESC). This reconfiguration would not only affect technical functions, but also high value-added occupations, support functions and coordination roles. The challenges posed in terms of training, retraining and recognition of hybrid skills could polarise the integration of workers, with a sharp increase in unemployment on the one hand and the introduction of a new form of work with alternative benefits and remuneration on the other.

2. Powerful collectives are formed to support and supervise the use of AI by society.
The social dimension of digital technology could grow given the considerable impact of AI technologies at the political level. Strong citizen mobilisations could emerge with the aim of providing structured support to the most vulnerable groups in their use of digital technology, in the most reasoned and responsible manner possible, around objectives relating to accessibility, sobriety and algorithmic transparency, among other things. These common interest groups could renew the collective commitment of former corporations and trade unions in a new spirit, capable of responding to the challenges of the Fourth Industrial Revolution. They would play an active and constructive role with public authorities, despite possible disagreements, in regulating digital practices.

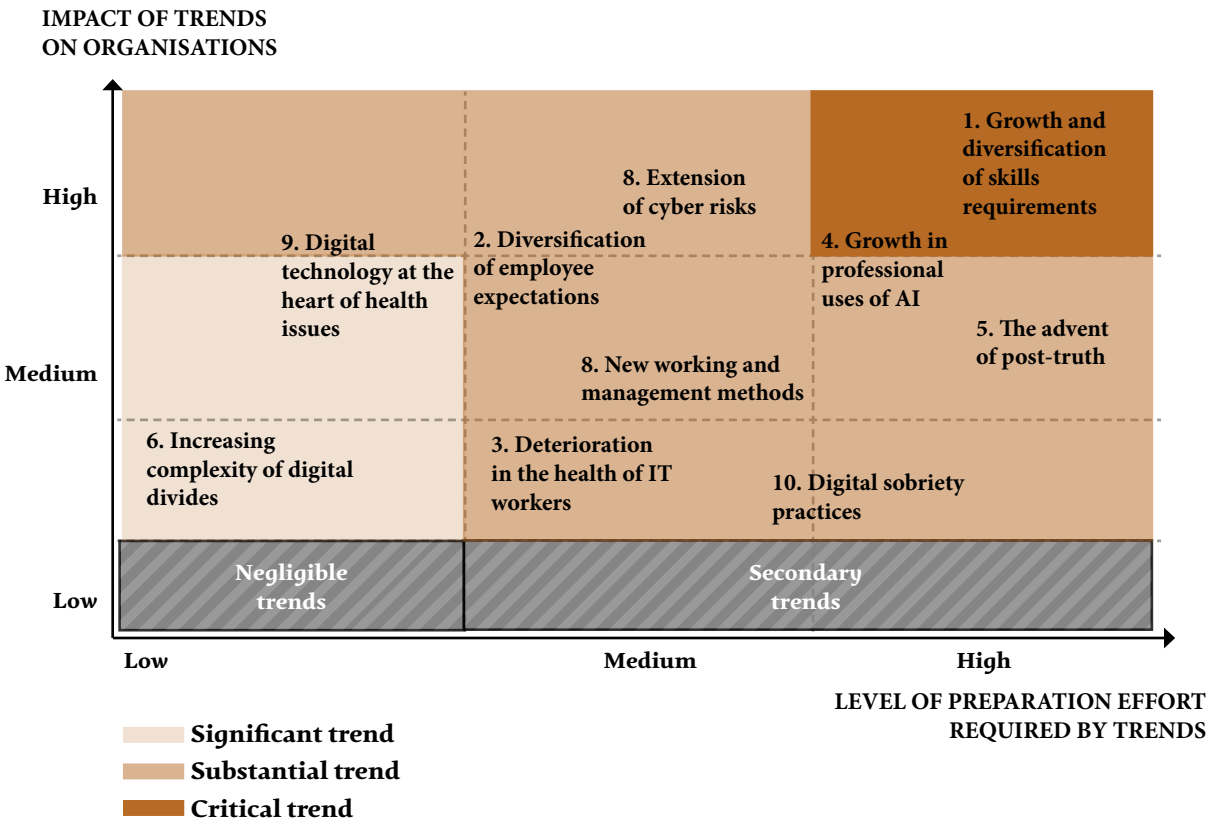
3. Part of the population finds itself excluded by new digital divides linked to the ability to use AI and understand its results.
The rapid spread of AI in everyday uses – public services, training, research, commerce – could make mastery of it essential. This increasing technicality could exclude part of the population, particularly those who are digitally excluded or poorly educated. The digital divide would not disappear, but would shift towards more subtle or inverted forms of the current digital divides, such as a divide with reality, linked to the inability to interpret, critique and use the results produced by AI, which has become ubiquitous.

4. Physical and mental health is deteriorating sharply as a result of the misuse of unregulated digital technology.
Without an awareness strategy or effective regulation, the omnipresence of digital technology from an early age could lead to a serious deterioration in the mental and physical health of those who are "left behind by digital technology". Screen addiction, attention disorders and socialisation problems would become so common that specific measures for this category of the population would be put in place in schools, organisations and healthcare centres.

5. A significant portion of the population rejects digital tools, either voluntarily or under duress.
As the negative impacts of digital technology become more widely recognised, there could be a voluntary or enforced reduction in screen use on a massive scale. This could lead to the emergence of a two-tier society, dividing those who are "connected" from those who are "disconnected", and reinforcing the challenges of social cohesion and the regulation of digital use.

Summary
Field 05 – Digital & Society

Major trends effort matrix



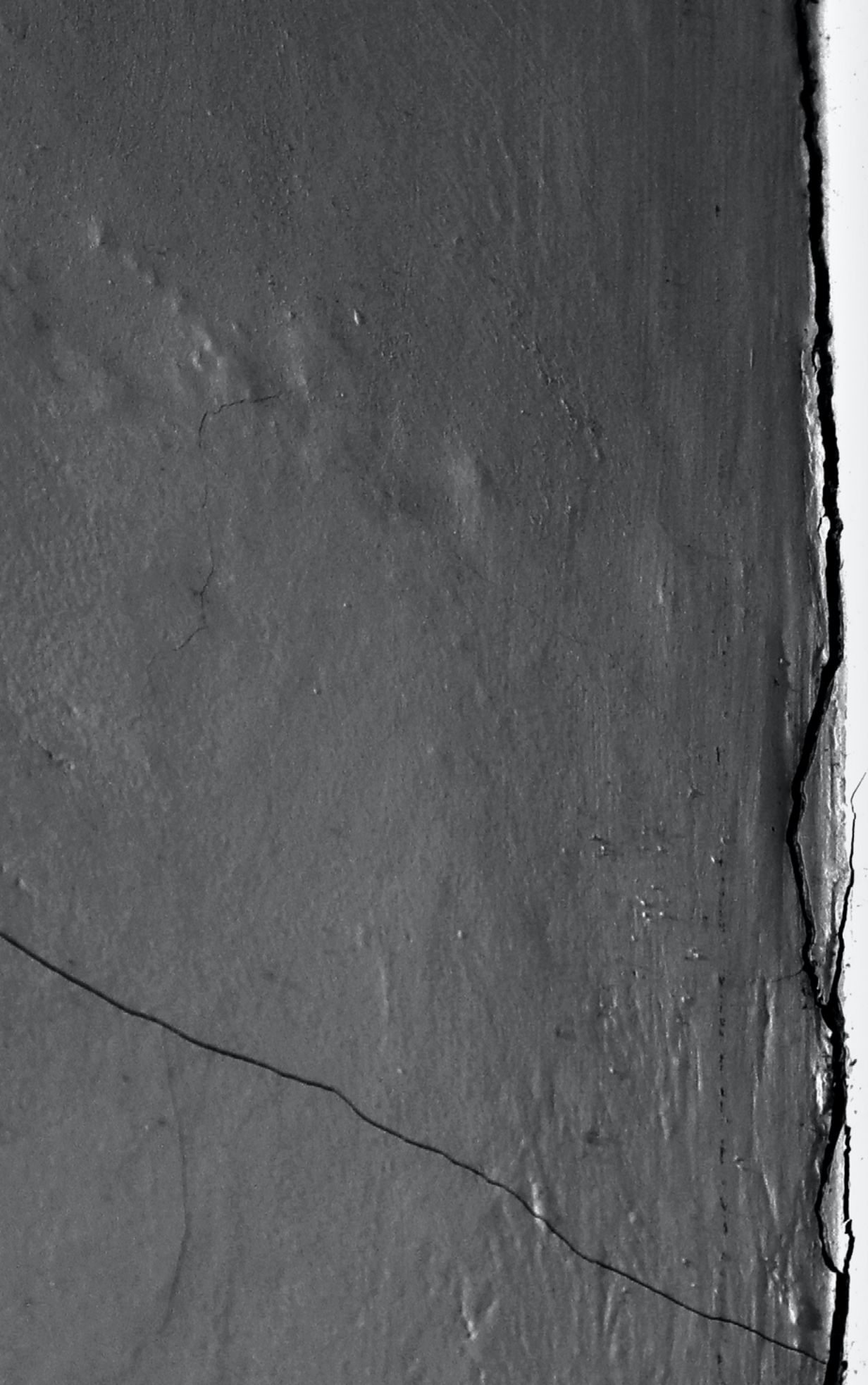
Reminder of the assumptions for disruptions by 2040

1. Advances in AI are leading to a profound reconfiguration of a large number of professions.
2. Powerful collectives are being formed to support and supervise the use of AI by society.
3. Part of the population finds itself excluded by new digital divides linked to the ability to use AI and understand its results.
4. Physical and mental health deteriorates significantly as a result of the misuse of unregulated digital technology.
5. A significant portion of the population rejects digital tools, either voluntarily or under duress.

Part 2

Archetypes of the digital function of the future

This second part explores possible futures for digital technology.



Archetypes of the digital function of the future

In the previous section, we attempted to envisage and understand the possible developments in the digital ecosystem. By analysing major trends and disruptive hypotheses, we sought to answer the question, "What might happen by 2040?" The aim was to anticipate the impact of current and future trends and the efforts they would require from organisations.

In this second part, we examined possible developments within IT departments themselves, in order to support reflection on the question "What could we become?" and to anticipate the opportunities that each organisation could derive from these transformations. The aim is to be able to envisage the future role and boundaries of the digital function.

The purpose of our forward-looking approach was therefore to identify archetypes of the digital function and describe their characteristics in order to inform organisations' strategic thinking. Four main archetypes have been identified and illustrated to embody the future diversity of the digital function. This typology aims to illustrate a few major models for 2040 that respond to internal transformations within organisations as well as changes in the geopolitical, economic, technological, environmental and social context.

To this end, a number of criteria have been identified that are characteristic of the digital function in organisations. These criteria can take different forms depending on the context and objectives pursued. The diversity of digital strategies also uses these criteria as variables, to be adjusted according to combinations specific to each organisation, depending on its core business activities, history and organisational culture. For each criterion, a series of hypotheses were formulated and then cross-referenced with each other in order to construct distinct and coherent models of the digital function of the future.

The archetypes proposed are, of course, neither normative models nor exclusive scenarios, and do not represent any particular organisation. They are primarily a basis for reflection, which digital departments can use to inform their strategic thinking. This will involve weighing up the opportunities and threats resulting from changes in the context against the strengths and weaknesses specific to each digital function. The archetypes reflect the different relationships that digital departments have with their organisations' overall strategy, the resources at their disposal, the technological choices they make, the stakeholders they engage and the sustainability issues they face. The emphasis is on the diversity of visions and possible trajectories among organisations rather than on the common goal to be achieved. On this basis, the relevance of each archetype can be questioned in order to identify strategic priorities and the associated levers for action.

In order to construct a realistic and cross-functional typology of archetypes, we selected ten criteria for which we identified different possible levels of positioning for the digital function. We then varied these criteria to cross-reference our hypotheses and identify typical profiles. Here is the main list, with the degree of appreciation of the digital function's positioning for each one:

- **Strategic role**: position of digital technology in business models and contribution to the organisation's overall strategy (support function, differentiating factor or fully integrated into core business activities).
- **Budget**: level of financial resources allocated to the digital function and its projects (reduction, stagnation, growth, explosion).
- **Project financing**: digital financing methods (internal, more or less decentralised by department, external and more or less exposed to pay-per-use pricing, public-private hybrids) and investment logic (short-term and long-term / incremental and disruptive innovation / return on investment, influence or environmental targeting).
- **Role of AI in activities**: degree of integration of artificial intelligence into business processes and decision-making (targeted at responsible, synergistic or ubiquitous uses).
- **Role of the cloud**: level of use of cloud technologies (public, private, national or European hybrid) for the digital infrastructures, products and services used.
- **Organisation of the digital function**: how the digital division or department operates (major programmes, agility of the project mode according to ad hoc requests, cross-functional and integrated contribution).
- **Management organisation**: work structure within digital teams (highly hierarchical, agile, autonomous, 100% remote working, etc.).
- **Team composition**: distribution of profiles (technical, functional, hybrid) and skills within digital teams.
- **Organisational variables with third parties**: development and management of digital assets (maximum delegation to external service providers, internalisation of critical skills and functions, limited number of partners or maximum derisking with numerous third parties).
- **Regulatory variables**: degree of supervision by applicable regulations and compliance approach (minimal, reactive, proactive).
- **Environmental variables**: consideration of environmental issues in technological choices, digital uses and governance (non-priority consideration, weighting factor and holistic design).

ARCHETYPE 1
The Lab

"The Lab" operates in a context of intense technological competition, marked by continuous acceleration of innovation and exponential growth in data.

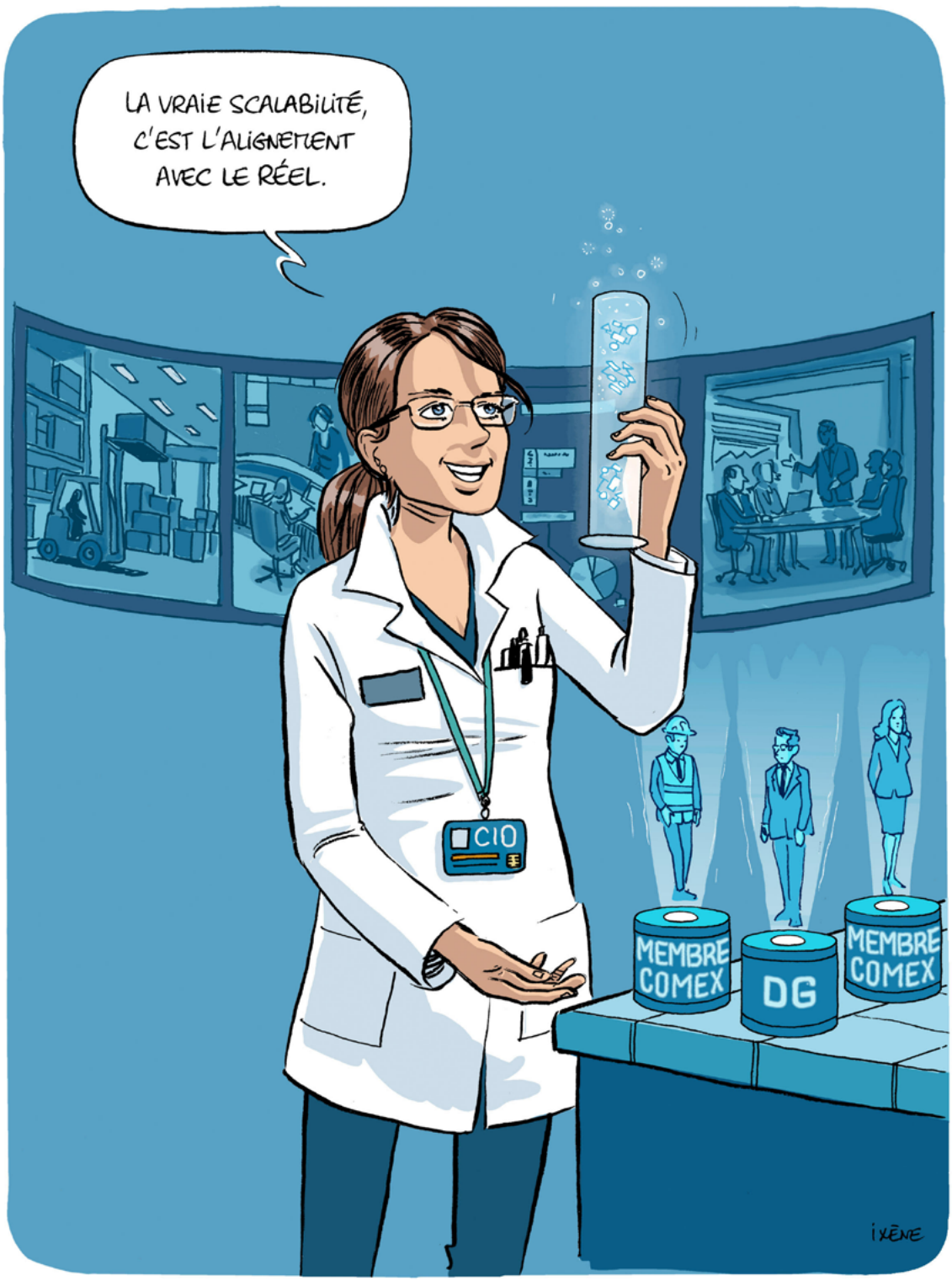
The Lab's priority is to expand the scope of digital technology, with the stated ambition of having a lasting impact on its immediate ecosystem. This strategic focus targets both internal stakeholders within the organisation, primarily its Executive Committee, and its peers in the digital sector, industry standards, public policy makers and citizens as digital users. Strongly integrated into the core businesses, the Lab is naturally positioned as a lever for competitiveness and contributes to the development and implementation of the organisation's strategy. Its proactive stance on regulations is reflected in its active participation in the co-construction of standards in sensitive areas and critical geographical zones.

Positioned at the heart of innovation, The Lab benefits from priority investments and strong growth. Firstly, a multi-year budget is set aside to anticipate disruptive innovations, complementing incremental innovation programmes and positioning the organisation as a competitor in key areas of its critical value chains. Secondly, a public relations strategy is implemented, particularly with governments, industry consortia and research laboratories, based on a controlled "coopetition" approach. Thirdly, vertical integration is driven by funds dedicated to acquiring equity stakes or buying out companies capable of creating a sphere of influence that is favourable to the organisation as a whole. The projects are based on hybrid financing arrangements (internal funds, grants, partnerships) aimed at maximising sectoral influence and ensuring measurable profitability.

The Lab is actively seeking strategic autonomy to navigate an unstable geopolitical environment by reducing its dependence on external suppliers and partially internalising its critical infrastructure. It has a particular ability to organise and represent its organisation's
its organisation's "diplomatic positions" in the digital sphere. Alignment and misalignment strategies are implemented and regularly reassessed in sensitive areas (cybersecurity, data transfer, interoperability standards). In addition, the fine segmentation of the multi-cloud reflects a strong capitalisation of intangible assets (data, algorithms, infrastructure), reconciling growth, resilience, scalability and sovereign and secure control of its projects.

The Lab's employees belong to an entity with an international reach. Their large-scale projects bring together interdisciplinary profiles, promoting agility and a digital approach that integrates its political and social dimensions. The decentralised organisation of work is based on strong cross-functional coordination, reinforced by the widespread practice of teleworking. **Tasks are largely automated by autonomous AI**, which goes beyond operational execution and participates in strategic decision-making, complex scenario simulation and supply chain management. **This dynamic of innovation, although effective, has a significant environmental impact**. Efforts are being made, but remain secondary to the imperatives of performance and speed.

INNOVATION MÉTIER ET EXPANSION DE L'INFLUENCE NUMÉRIQUE



ARCHETYPE 2
The Chameleon

The Chameleon operates in an environment characterised by rapid technological change, increasing consumer expectations and constant pressure to meet implementation deadlines.

Its strategic positioning is based on the scalability of solutions, adaptability and organisational agility, drawing on strong skills in change management and project management. Although inseparable from business strategy, Le Caméléon is still perceived as a support function, reactive and available on demand, like a temporary IT department or a team of digital 'firefighters'. In regulatory terms, it operates in areas of lesser constraint, with a reactive rather than proactive stance towards standards. However, it ensures minimum compliance on critical aspects (GDPR, data security) without hindering innovation.

Le Caméléon draws a comparative advantage from its ability to respond quickly to business needs, focusing primarily on integrating new technologies and improving business skills in existing solutions. Projects are often short-term, geared towards concrete and measurable results. Budgets are increased for digital transformation initiatives, which are seen as direct drivers of performance and competitiveness. Funding is decentralised, with local decision-making and a focus on rapid return on investment.

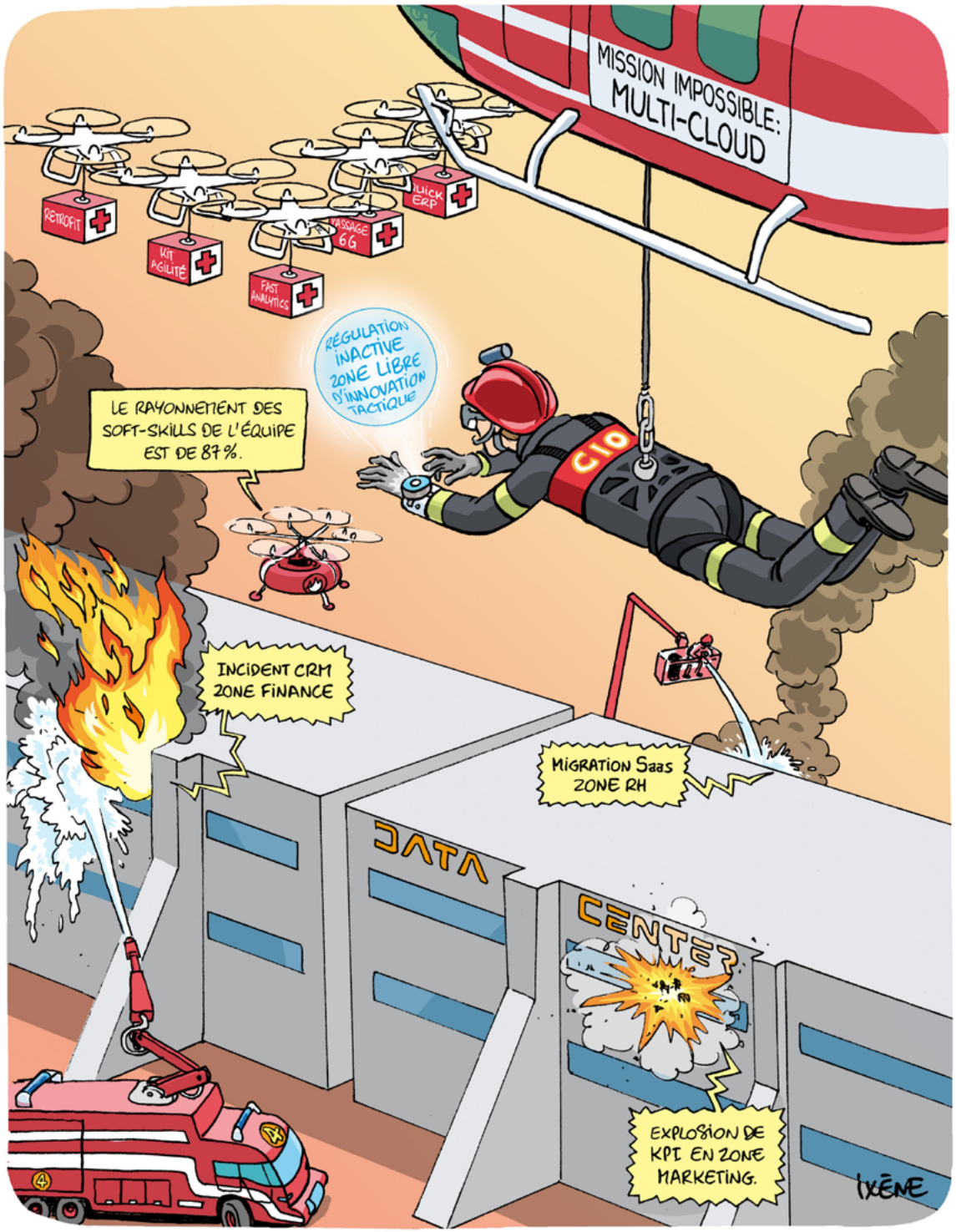
Work organisation is entirely flexible, with distributed, autonomous and project-oriented teams. The model is based on strong involvement in the early stages of projects, with surgical targeting of objectives, rapid identification of levers for improvement and the ability to deliver within tight deadlines. Efficiency and financial resilience are the watchwords, driven by an active strategy of technological and organisational diversification. The adoption of SaaS solutions is the norm, and the technological dependencies that these activities create are offset by heavy investment in multi-cloud projects to promote reversibility and interoperability.

The project method is inspired by management practices used by special forces. In this regard, Le Caméléon has a dual capacity to initiate or halt a project (start S stop) on the one hand, and to move from one strategic issue to another without dwelling on it (first-in, first-out) on the other. Talent recruitment focuses on hybrid profiles, project managers, integration experts, functional consultants and user adoption specialists.

AI is integrated to enhance human capabilities, automate repetitive tasks and streamline processes. Particular attention is paid to reversibility and interoperability, through multi-cloud projects that can be pivoted very quickly. This approach limits technological dependencies while ensuring maximum agility.

Environmental issues are taken into account primarily from a utilitarian perspective. The flexibility of the model allows for the integration of more energy-efficient solutions when compatible with performance objectives. Teleworking and the dematerialisation of processes help to limit the carbon footprint, although this has not yet been fully integrated as a strategic priority in its own right.

RÉSILIENCE ORGANISATIONNELLE ET TRANSFORMATION TACTIQUE DU CHAOS NUMÉRIQUE



ARCHETYPE 3
The Stewards

The Stewards operates in a context of increased pressure in terms of energy trade-offs and environmental dependencies, coupled with strong stakeholder demands for digital sustainability.

Its strategic positioning incorporates the management of systemic environmental risks as a key guiding principle, shaping technological choices, business models and investment priorities. Priority is given to sustainability, integrating ecological, social and territorial issues into the design, deployment and governance of information systems. On the regulatory front, the Stewards adopts a proactive stance, anticipating regulatory changes and contributing to their operational implementation. It integrates environmental issues into its performance indicators, dashboards and technological decisions.

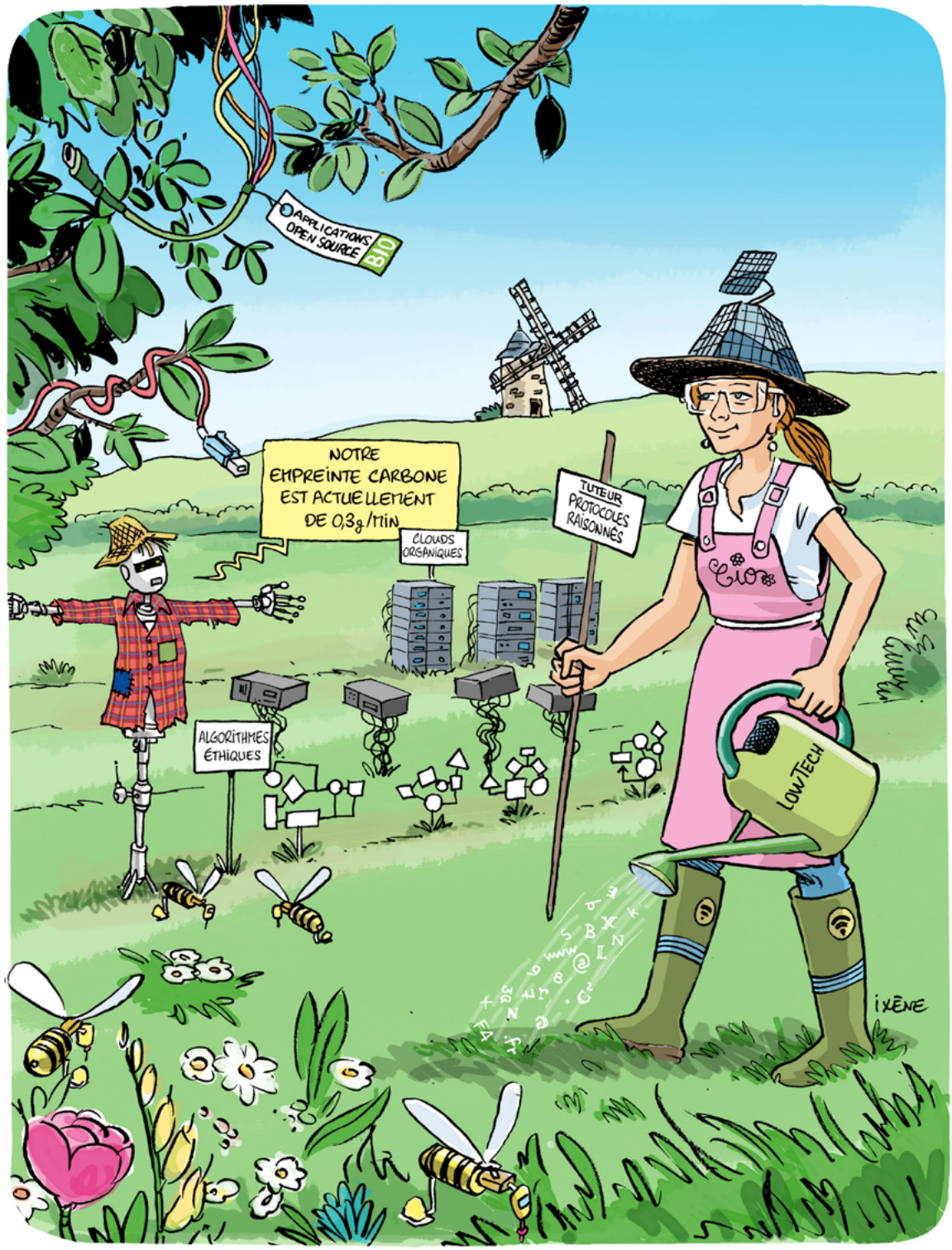
The Stewards has a unique ability to think in terms of ecosystems and act holistically. It develops a clear vision of the positioning and influence of stakeholders in an ecosystem that has become volatile, uncertain, complex and ambiguous. Particular attention is paid to studying the impact of digital activities on the organisation's own ecosystem, as well as the technical resilience of its infrastructure across all critical phases of its value chains.

Within the Stewards, the challenge of making digital technology a driver of energy transition is reflected in an innovative approach to performance: "Green IT as a Service". At the heart of the business and as an internal economic partner, the Stewards acts proactively as a true catalyst for green innovation. It is able to offer its services to external clients when the maturity, social interest of the projects, and availability of skills allow it. To combine operational performance and digital sobriety, investments are primarily allocated to projects that reduce the effects of climate change and have a low ecological footprint: shared infrastructure, open source software, material recyclability, low-tech solutions, and frugal AI. Project financing is often mixed, combining internal resources, public support mechanisms for sustainable innovation, and regional partnerships.

The recruitment of employees reflects the company's focus on digital resilience, bringing together technical experts, environmental specialists, sustainable service designers and regulatory advisors. The organisation of work is highly decentralised, with a hybrid model that limits travel and reduces the carbon footprint. Governance is flexible and demanding, based on individual responsibility and co-construction with stakeholders.

AI is used in a reasoned manner, with particular attention paid to energy consumption, model traceability and their contribution to the common good. The Cloud is used selectively, with a preference for shared, sovereign or low-energy solutions.

CULTURE NUMÉRIQUE ET MAÎTRISE DE SON ÉCOSYSTÈME RÉSILIENT



ARCHETYPE 4
The Resourceful

The Resourceful operates in an unstable global environment marked by geopolitical tensions, growing cyber risks and persistent budgetary constraints. In this context, it adopts a stance focused on robustness, operational resilience and business continuity.

Its strategic positioning is the result of optimising constraints, particularly financial and security constraints. The Resourceful fully assumes the role of a support function on which business lines can rely with confidence and reliability. In regulatory terms, it adopts a rigorous compliance stance, often reactive, but structured around solid benchmarks. Risk management is at the heart of the Resourceful's performance, which incorporates monitoring and surveillance, traceability and remediation mechanisms, while relying on human vigilance to prevent the continuum of digital threats (informational, cognitive and cyber).

Its main objective is to ensure business continuity through robustness, by securing digital architectures, products and services. A significant portion is co-developed with a limited number of trusted software publishers, within a long-term partnership approach. Investments target critical stages in the various value chains and aim to reduce external dependencies. Funded mainly by internal resources, the Resourceful optimises costs and pools its digital assets as much as possible. Digital budgets, relative to overall budgets, are certainly modest, but they are mobilised with great rigour and inventiveness.

The Resourceful makes risk management an essential part of its performance. The organisation is centralised and structured around a close-knit and supportive team, which has made the principle of trust a cornerstone of its operations. The human factor (know-how, interpersonal skills) is the focus of great attention. The knowledge acquired through experience of past events and incidents, the ability to discern weak signals, and prudent and nuanced judgement are all human skills valued by the Resourceful as levers for efficiency and asset security. The operating mode favours proven practices, technical education and interpersonal trust, rather than a techno-solutionist approach.

The Resourceful is mainly composed of specialist technical profiles, with strong expertise in critical systems, technical and financial optimisation, and incremental innovation. The organisational approach does not use a matrix organisational model or particularly cross-functional management, and a return to face-to-face working is encouraged to strengthen operational control, streamline information sharing and promote collective training in technical skills on a daily basis.

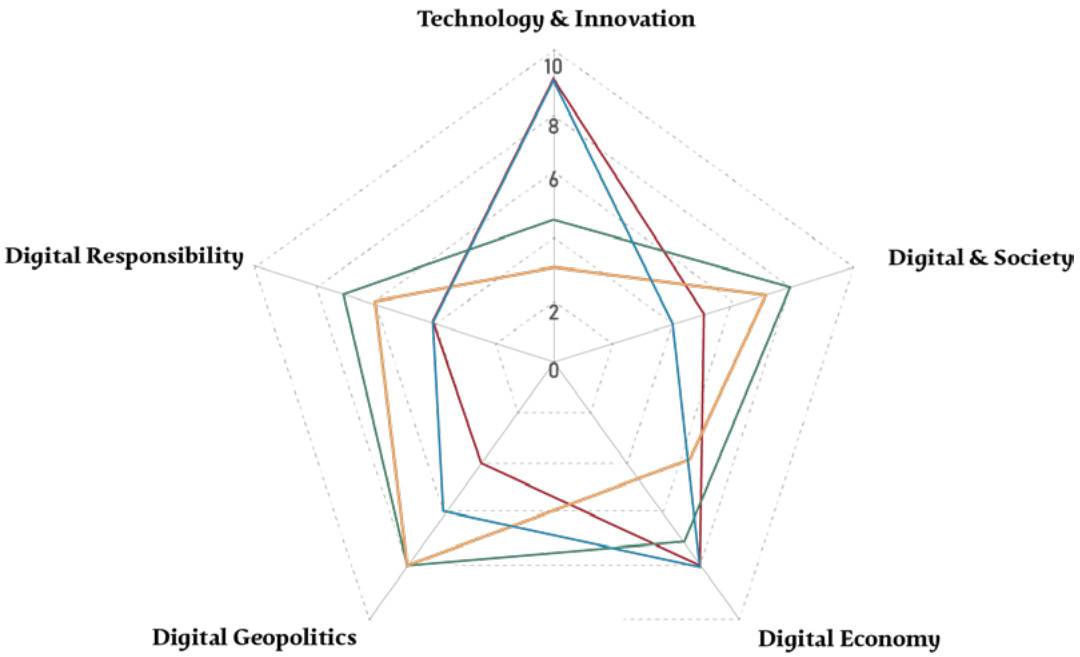
Within the Resourceful, AI is used in a targeted manner, mainly to automate repetitive tasks at low cost or reduce costs by drawing on increased expertise acquired, transferred and consolidated internally. The Cloud is used selectively, with a preference for private or sector-specific solutions, in order to guarantee risk control and data sovereignty. **Environmental issues are taken into account in a pragmatic manner**, with a focus on equipment sustainability, streamlining flows and sober usage.

RÉSILIENCE OPÉRATIONNELLE ET SOLIDARITÉ DIFFUSE

Summary

Archetypes of the digital function

Strategic positioning of archetypes



1. The Lab
Focused on expanding the prerogatives of digital technology, with the ambition of having a lasting influence on its direct ecosystem based on a strong concept of strategic autonomy.

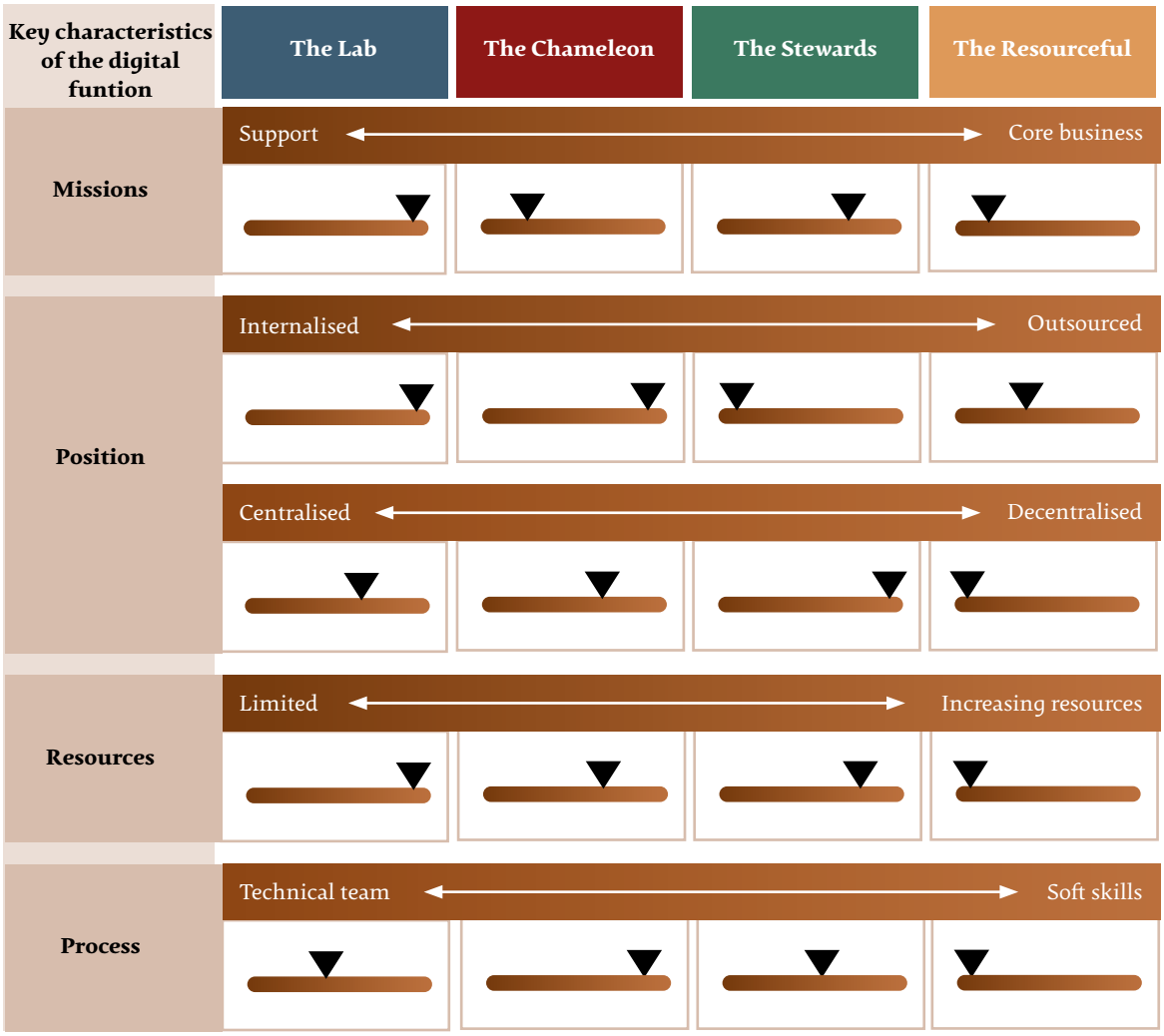
2. The Chameleon
Focused on solution scalability and organisational agility, leveraging its rapid adaptation to business needs.

3. The Stewards
Anchored in the management of systemic environmental risks, taking up the challenge of digital technology as a driver of energy transition, in the service of innovation and performance.

4. The Resourceful
Structured around optimising constraints, prioritising operational resilience through robustness, efficiency and service continuity.

Functional evaluation of archetypes

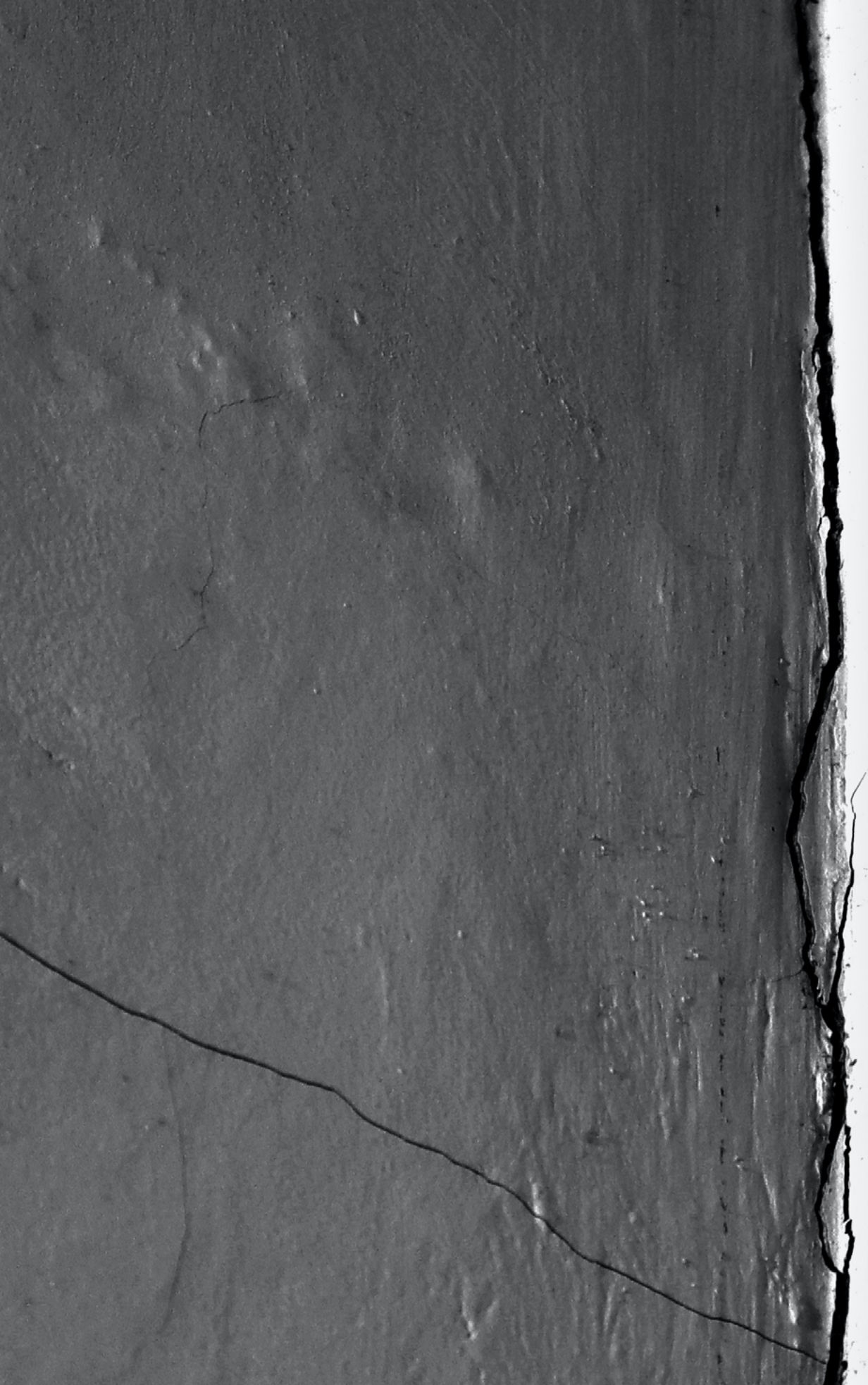
For each key characteristic of the digital function, the table presents the evaluation of the archetypes according to five assessment criteria (support/core business, internal/external, centralised/decentralised, limited resources/growing resources, technical team/soft skills).



Part 3

Principles of Strategic Action

This final part proposes a set of principles for preparing for future transformations, linking forward-looking research and concrete actions.



Principles for strategic action

This last section proposes ten principles for action *identified to move from prospective research to concrete implementation, by projecting trends to the year 2040 and constructing archetypes of the digital function of the future. These elements aim to help organisations, and in particular their digital departments, prepare for the transformations to come.*

01 Digital Geopolitics

Principle of action 1. Proactive resilience

"By 2040, proactive resilience will become an asset in ensuring service continuity in the face of international crises."

As geopolitical tensions multiply, intensify and upset the global balance, the ability to proactively consider the opportunities for progress that arise from crises should be a differentiating asset for organisations.

Taking geopolitical risks into account at the highest level of governance is essential as a first step. The process of mitigating risks is also indispensable and involves, in particular:

- **The definition of a maximum threshold for** operational **risk acceptability.**
- **Mapping technological dependencies** across all critical value chains (infrastructure, hardware, software, services, data).
- **Measuring the degree of substitution** of IT purchases.

This mindset would benefit from being disseminated at the individual employee level to make the human factor a bulwark against the continuum of digital threats (cyber, informational and cognitive). Its scope could be reinforced by the creation within organisations of an IT monitoring and forecasting entity that promotes the consideration of geopolitical risks in all decision-making and operational processes. Defining a target level of resilience could then become a major strategic factor, guiding the production of geopolitical risk scenarios and facilitating the prioritisation of responses in times of crisis and calm.

Principle of action 2. Strategic autonomy policy

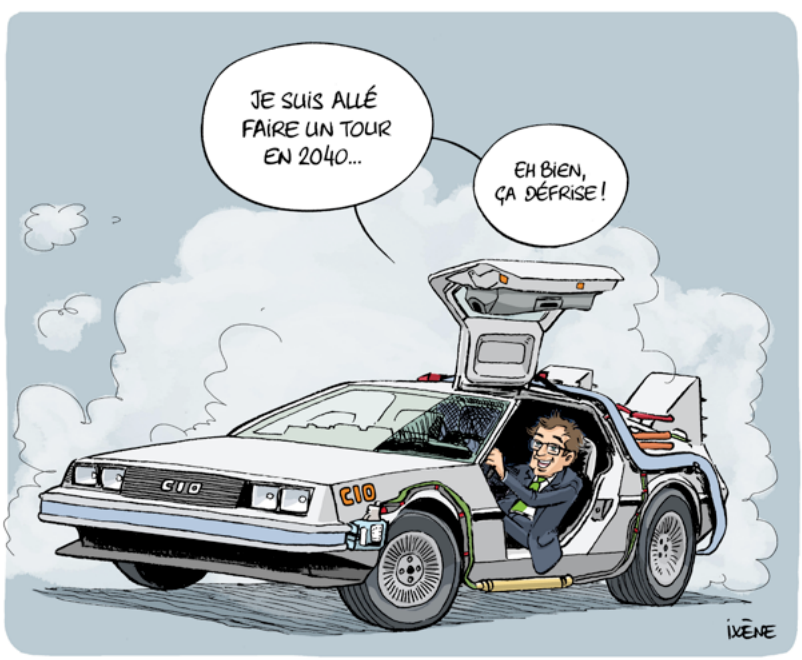
"By 2040, the politicisation of digital activities, whether imposed or voluntary, will make it necessary to clearly define an internal policy of strategic autonomy."

A relative questioning of institutions and international law has been observed over the past decade. If this trend continues, the pursuit of strategic autonomy could become a necessary condition for competitiveness and freedom of action in a global environment undergoing reconfiguration.

Support from national and European public policies on public procurement, European preference, tax and investment provisions, immunity from the extraterritorial reach of non-European laws, and regulation of activities in the broad sense could significantly accelerate and strengthen the strategic autonomy policies of European organisations. This support could also help to stem the fragmentation of international relations, in which each economic actor would have to bear the burden of its own diplomatic line alone.

To address the growing politicisation of digital technology, organisations could mobilise various levers:

- **Identifying the risks associated with geopolitical phenomena** affecting the availability, integrity and confidentiality of systems and data.
- **Diversifying suppliers, third parties and partnerships** for IT procurement in order to minimise the risk of supply disruptions in the event of a diplomatic crisis.
- **Strengthening cyber diplomacy** (cyber ambassadors, enhanced CERT-EU) and operational cooperation (sectoral resilience strategy, pooling of sovereign SOCs).



02 Digital Economy

Principle of action 3. Rebalancing value chains

"By 2040, the growing regionalisation of infrastructure, standards and regulations will require a de facto rebalancing of value chains."

Regulatory fragmentation and accelerating economic tensions are likely to prompt organisations to anticipate numerous reconfigurations within digital value chains. The regionalisation of infrastructure, standards and regulations may no longer be a matter for institutional debate, but rather an operational imperative for business continuity and economic performance.

In order to benefit from credible, large-scale alternatives on the European market, organisations could be encouraged, in conjunction with governments, to structure their investments in technological capital, in particular by:

- **Mobilising private funds** to facilitate equity investments, European buyouts and the pooling of targeted initiatives by European business angels offering real added value.
- **Establishing incentives and restrictions for financing** innovative companies and projects in order to curb as much as possible the flight of capital and brains outside the European area.
- **Supporting the emergence of regional champions through public procurement** complementary to private procurement, through co-innovation and through partnerships targeting the maturity and scale of organisations.

By 2040, only a strategy of industrial and regulatory alignment will be able to secure the long-term digital performance of organisations, in line with the European social model.

Principle of action 4. Contractual flexibility

"By 2040, contractual manoeuvrability will be a key factor in reducing technological dependencies."

Reducing the impact of technological dependencies on organisations' business models should be a major focus by 2040.

Economically speaking, contractual flexibility and clarity could become two key levers for budgetary control, targeting strategic investments more effectively, with a particular focus on the following elements:

- **The portability and interoperability of the digital solutions and services used**, the specific features of which could be referenced by a framework for evaluating and recommending offers, established at European level.

- **Sequencing contractual commitments over different time horizons**, distinguishing between critical, highly sensitive services (data, security, cloud, AI) and more generic functions. Organisations could choose between short-term frameworks, favouring flexibility, and long-term frameworks, guaranteeing stability, while retaining room for manoeuvre to reassess their choices.
- **The integration, from the negotiation phase onwards, of a costed exit plan, as well as one or more contingency plans**, updated regularly, in order to facilitate supplier diversification and limit lock-in effects. This approach would strengthen organisations' ability to adapt to regulatory changes and cyclical fiscal policies, technological disruptions or changes in the sovereignty of service providers.

03

Principle of action 5. Mastery of AI technologies

"By 2040, mastery of the various components of AI technologies will become an operational requirement."

The generation of autonomous content and the structuring of automated AI-to-AI action chains should continue to generate fascination and widespread adoption. However, operations carried out by AI technologies require an ecosystem that is conducive to their proper functioning and use on an industrial scale. The responsible and transparent integration of these functionalities could pose a challenge on several levels:

- **The qualification of input datasets**, or active protection in the form of watermarking capable of "modifying content imperceptibly while inserting a mark proving that the content is generated"1.
- **The continuous supply of "fresh" data** to maintain a connection to reality, with deterministic and unique validation at the output in order to avoid the depletion and degradation of information in a closed circuit.
- **Monitoring the compliance of interactions between artificial agents**, or ensuring the ongoing explainability of software and maintaining employee skills in line with changing job descriptions.

This process could be strengthened through cooperation with European players who share the same culture of innovation and entrepreneurship, and through European legislation that makes these practices a market requirement.

Principle of action 6. Ability to create ecosystems

"By 2040, the ability to build ecosystems will become an essential lever for guiding and supporting technological innovation."

By 2040, the development of spaces, products, services or technological layers could represent budgets so large that only a few players would be able to pass on their financing costs to prices and end consumers.

The technological competitiveness of organisations could depend on their ability to structure their innovation around different axes:

- **A culture of cooperation and "intrapreneurship"**, combining a digital strategy driven by the Executive Committee and technological initiatives from various departments.
- **Broader and deeper collaboration with other trusted players in the digital ecosystem** (businesses, government agencies, research organisations, professional associations, CSF, etc.) to strengthen the realism and resilience of "Make or Buy" strategies and support alternative solutions, such as open source.
- **The identification of sectoral channels for using collaborative spaces with shared governance and semantics**, capable of establishing standards and ensuring legal and technical interoperability.

04 Digital Responsibility

Principle of action 7. Anticipating resource trade-offs

"By 2040, public-private dialogue on virtuous French and European regulations will become a key factor in the digital environmental resilience of organisations."

In a context of increased ecological constraints, digital environmental resilience could become an operational requirement that directly influences technological choices. Digital functions, considered critical infrastructure, should integrate climate engineering measures that take into account resource management, greenhouse gas emissions and ecosystems in order to combine performance, sustainability and robustness.

This transformation could be based on three principles of action:

- **The native integration of insurability and sustainability indices** into the financial design of digital projects, to anticipate climate hazards and ensure business continuity.
- **Adapting technical architectures and geographical locations** in response to physical risks and pressure on energy resources.

- **The structuring of a demanding regulatory framework** based on public-private dialogue. This framework would offer stability, visibility and targeted incentives to encourage long-term investment by organisations and make Digital Responsibility a lever for competitiveness, legitimacy and industrial sovereignty. This constructive dialogue would also enable organisations to anticipate the effects of future regulations, such as possible recyclability quotas or usage restrictions, by integrating them into a map of national and regional policy trade-offs.

This framework could enable French organisations to redefine the conditions for sustainable technological progress at European level, aligning digital innovation with planetary boundaries.

Principle of action 8. Environmental resilience of business models

"By 2040, energy optimisation and the use of more sustainable materials in the digital sector will be an integral part of business models."

Growing pressure on resources, critical supply chains and energy infrastructure is likely to accelerate a reconfiguration of the physical foundations of digital technology. Aligning strategic decisions with operational practices could reinforce the focus on the environmental impact of digital technology in CSR reports, management committees, performance monitoring tables and HR acculturation practices, with a focus on self-regulation of high-impact uses. To address issues of storage capacity, equipment lifespan and manufacturing costs, eco-design of equipment, energy efficiency of components, diversification of materials and partial relocation of material production could become industrial imperatives. This evolution could be structured around three concrete drivers, based on the principles of the circular economy:

- **The development of alternative materials to rare earths**, such as graphene, conductive polymers or organic semiconductors, to limit dependence on critical resources.
- **Reducing the energy footprint of digital components and solution**s by improving upstream design and manufacturing processes (lower firing temperatures, advanced 3D printing) for more energy-efficient chips and by promoting downstream open-source, frugal and sustainable solutions, including those based on artificial intelligence.
- **Structuring recycling and repairability channels**, with modular equipment that is more durable over time. Organisations could strengthen their partnership strategies with players in the reconditioning, reuse and repair sectors, including internally.

These transformations could be accelerated by European industrial cooperation, targeted regulatory incentives and an innovation policy geared towards technological sustainability.

05 Digital Responsibility

Principle of action 9. Sustainable use of AI technologies

"By 2040, supervision and support for the sensible use of AI technologies will become essential to making human-machine complementarity a source of sustainable organisational performance."

The rapid and often spontaneous adoption of AI technologies in professional environments is expected to transform work practices, organisational models and governance balances. While their contributions to productivity and cognitive assistance are recognised, their unregulated use is likely to continue to expose organisations to growing risks in terms of health, social cohesion, the environment and cyber risks. The synergistic and reasoned integration of AI technologies could be based on three strategic pillars:

- **The definition of clear internal policies** promoting the use of AI within a specific framework for task optimisation, with authorised tools and associated responsibilities, in order to limit grey areas and ensure regulatory compliance. Training and promoting appropriate, targeted uses that comply with organisational policies should represent a powerful strategic asset.
- **The development of targeted and personalised support programmes within organisations**, aimed at growing, maintaining and strengthening skills that complement AI: logical reasoning, ethical judgement, prioritisation of ideas and impact assessment.
- **Anticipating changes in the labour market and the digital sector** through proactive management of career paths (continuing education, skills development, career transitions), adapting pay scales to the most humanly valuable tasks, and monitoring new emerging roles.

Principle of action 10. Promoting digital skills

"By 2040, the ability of organisations to anticipate digital skills needs and structure agile training pathways will become a key driver of organisational resilience."

The sustained growth of the digital sector, combined with technological acceleration, is likely to require a substantial restructuring of the labour market, at a time when the digital sector is already experiencing both quantitative and qualitative recruitment pressures. In a challenging demographic context, organisations' HR strategies could focus more specifically on finding, developing and retaining the key skills they will need.

To overcome the talent shortage, increased specialisation of skills and rapid changes in professions, this transformation could be based on three key drivers:

- **Structuring agile and personalised training programmes**, incorporating internal mobility, upskilling or reskilling to respond to the continuous evolution of job descriptions.
- **Promoting diversity and hybrid skills, combining** soft skills, bot-to-bot design and customer experience, human sciences and fundamental research, IT strategy and technical governance, risk management, data intelligence and engineering.
- **Strengthening regional and academic cooperation** between educational institutions, centres of research excellence and organisations to make digital technology a vector for human development.

The most mature organisations could take on the role of "orchestrators of human development", making HR resilience a differentiating factor in attractiveness, legitimacy and managerial innovation.

Members of the Strategic Steering Committee

Cigref members

Lionel CHAINE - BPI FRANCE
Jean-Claude LAROCHE - EDF
Franck LE MOAL - LVMH
Emmanuel SARDET - CRÉDIT AGRICOLE
Laurent TRELUYER - CNAF

Qualified individuals

Yves BERNAERT - 1001FONTAINES
Suzy CANIVENC - MINES PARIS
Cécile MEADEL - UNIVERSITÉ PARIS II - PANTHÉON ASSAS
Julien NOCETTI - IFRI
Arno PONS - DIGITAL NEW DEAL FOUNDATION

Members of the Youth Strategic Advisory Board

Established in 2023, the Youth Strategic Advisory Board is made up of 71 employees under the age of 30 from 40 Cigref member organisations.

AIOUAZ Selma - FONDATION DE FRANCE
ALMON Mathieu - MSA
AMMAR Dhia Eddine - CNAM
AMRANI Thoraya - AGIRC ARRCO
ASNACIOS Youri - MINISTÈRE DE LA TRANSITION ÉCOLOGIQUE
AUDRAN Thomas - GROUPE SAVENCIA
AZZOUG Pierre-Edouard - MINISTÈRE DE L'INTÉRIEUR
BERMOND Lisa - AIRBUS
BERNARDIE Jade - MINISTÈRE DES ARMÉES
BERNARDO Christelle - MINISTÈRES SOCIAUX
BESBES Makram - INVIVO
BIGANT Etienne - BRED
BIHAN Alexis - GROUPE SAVENCIA
BINEL Oann - CNES
BOUDET Thomas - DASSAULT AVIATION
BOURSAULT Maloya - FRANCE TRAVAIL
BOUSSAHABA Marvin - BANQUE DE FRANCE
CALVIER Mickaël - AGIRC ARRCO
CAO Caroline - SOCIÉTÉ GÉNÉRALE
CELOSIA Guillaume - GROUPE SAVENCIA
CHAUMES Billy - CNES
COVILLE Romain - ENGIE
DAVRIL Geoffrey - MINISTÈRE DES ARMÉES
DAYAUX Guillaume - ESSILORLUXOTTICA
DELAUNAY Clément - SODEXO
DUPONT Thibault - AIRBUS
ECHELARD Camille - DASSAULT AVIATION
FILICHKINA Alena - SODEXO
FORET Gabriel - AG2R LA MONDIALE
FOUILLE Justine - GROUPE EGIS
GAO Lise - ERAMET GROUP
GERMÉ Allan - AG2R LA MONDIALE
GODART Arthur - THALES
GRESSET Erwan - MSA
HAMON Fanny - MINISTÈRE DE L'INTÉRIEUR
JEMETZ Maël - HARMONIE MUTUELLE
KAYTMAZ Pelin - ORANGE
KOBEISSI Victor - AXA
LALLEMENT Julie - AG2R LA MONDIALE
LAVANANT Clément - MINISTÈRES SOCIAUX
LAVODRAMA Muriel - AIR FRANCE-KLM
LEFRANCOIS Alexandre - FRANCE TRAVAIL
MARILLEAU Mallik - COVÉA
MARQUES Charlène - MINISTÈRE DE L'INTÉRIEUR
MARTINS GONCALVES Amandine - BNP PARIBAS
MAZARS Alexandre - ABEILLE ASSURANCES
METAYER Pauline - EIFFAGE
MILLEVILLE Camille - LVMH
MORESCO Maxime - ARKEMA
NAKOTE Tibé-Pakyendou - MSA
NGUYEN Tich Bao - SOCIÉTÉ GÉNÉRALE
PEDINOTTI Thomas - ABEILLE ASSURANCES
RAMSAMY Cyril - AIRBUS
REBOUL SALZE Noël - ABEILLE ASSURANCES
REBULLIOT Bastien - GROUPE ROCHER
RICHARD Solène - AIR FRANCE-KLM
ROBIN Arnaud - DINUM
SEBAH Carole - DASSAULT AVIATION
SECHIER Hugo - STELLANTIS
SILVA VIEIRA Lorena - ORANGE
TORRES Franck - MSA
TOUATI Clément - AIR FRANCE-KLM
VESVAL Clara - AGIRC ARRCO
WASCAT Delphine - MSA
ZAID Amina - BNP PARIBAS

Acknowledgements

Cigref would like to warmly thank the members of the Strategic Advisory Board, the Youth Strategic Advisory Board and all Cigref members for their rich and stimulating contributions.

For the sixth consecutive year, we would also like to thank the team at Futuribles, Cigref's long-standing partner, for their support in developing this forward-looking vision. This report, intended primarily for Cigref members, is also aimed at the entire digital ecosystem and anyone interested in digital issues and a multidisciplinary, forward-looking approach to them.

Editorial team

Pierre Skrzypczak, Senior Project Manager
Henri d'Agrain, Chief Executive Officer

In collaboration with Futuribles

François de Jouvenel, Director
Cécile Désaunay, Director of Studies
Juliette Guilbaud, Research Officer

Contributions from the Cigref team: Aymeric Bourdin, Célia Culi, Flora Fischer, Frédéric Lau, Marine de Sury, Elena Silvera

Proofreading: **Chantal de Bardies**, Director of Content, Cigref

Artistic direction and communication: **Émilie Grange**, Communications Officer, Cigref

Original illustrations: **Ixène** (https://www.instagram.com/ixene/)

This report was produced by HandiPRINT, a company that employs 120 people with disabilities in the comprehensive management of printed documents. For more information: www.handi-print.fr

Cigref
www.cigref.fr
21 avenue de Messine, 75008 Paris
+33 1 56 59 70 00
cigref@cigref.fr