INSTITUTE
OF ECONOMICS

Scuola Superiore
Sant'Anna

LEM | Laboratory of Economics and Management

Institute of Economics
Scuola Superiore Sant'Anna

Piazza Martiri della Libertà, 33 – 56127 Pisa, Italy
ph. +39 050 88.33.43
institute.economics@sssup.it

LEM
WORKING PAPER SERIES

Technological Sovereignity, Big Tech and the Military-Digital complex

Francesco Crespi [1]
Dario Guarascio [2]
Jelena Reljic [2]

[1] University of Roma Tre, Italy Italy
[2] Sapienza University of Rome, Italy

2026/20 **June 2026**

ISSN(ONLINE) 2284-0400
DOI: 10.57838/sssa/exxw-mf60

Technological Sovereignity, Big Tech and the Military-Digital complex

Francesco Crespi – *University of Roma Tre*

Dario Guarascio[*] – *Sapienza University of Rome*

Jelena Reljic – *Sapienza University of Rome*

Abstract

This article reassesses the concept of technological sovereignty and its policy implications in light of the close relationships between US- and China-based digital monopolies (i.e., Big Tech) and their respective military apparatuses. First, we empirically examine the growing influence of the private sector in R&D activities, the increasing centrality of digital technologies within sectoral and technological hierarchies, the emergence of Big Tech firms and their dominance over knowledge, infrastructures, and key technologies such as cloud computing and AI. Second, building on Coveri et al. (2025a), we analyse the mutual dependence between Big Tech and the military apparatus, showing how it reinforces the economic power of the private actors involved, weakens the state's capacity to act autonomously, and intensifies the subordination of foreign governments dependent on US and Chinese digital platforms. Third, we propose a typology of technological sovereignty that takes into account the degree of technological dependence on Big Tech, the nature of the relationship between states and digital companies, and, consequently, the state's capacity to align the activities of these companies with its own strategic objectives

Keywords: technological sovereignty, Big Tech, R&D, military apparatus.

JEL codes: F5, F52, F55, O33, O34, O38.

1. Introduction

As trade, technological, and military conflicts accelerate the fragmentation of the global economy and heighten uncertainty, the concept of *technological sovereignty* (TS) is gaining prominence in scientific and policy debates alike (Crespi et al., 2021; Edler et al., 2020, 2023). Investment decisions and the international division of labour are gradually moving away from cost minimisation and efficiency-related considerations; to be increasingly driven by the need to produce, access, and control key technologies in order to avoid one-sided dependence on foreign actors (Andreoni and Chang, 2019). This implies a major policy shift: from horizontal (sector-neutral) industrial policies towards strategic/vertical interventions (e.g., import substitution and direct support to 'national champions') aimed at selecting sectors, strengthening critical supply chains (e.g., semiconductors, lithium batteries, pharmaceuticals) and building technological capabilities in areas deemed key to address systemic challenges such as decarbonisation and digitalisation (Caravella et al., 2024).

In this context, TS refers to the ability of a nation state (or a federation of states) to access and provide technologies that are critical for welfare and competitiveness 'without incurring in one-sided structural dependency' (Edler et al., 2023). While this approach highlights a crucial evolution in industrial and innovation policy, it partly overlooks a defining feature of contemporary capitalism: the systemic power of major US and Chinese digital companies, or 'Big Tech' (Cirillo et al., 2025). The latter epitomises a broader structural trend in which global economic and geopolitical relations are increasingly shaped by technological dependence on a handful of companies that control key infrastructures, technologies, and knowledge essential to the functioning of most public and private activities. This paper examines how such an unprecedented concentration of techno-economic power reshapes the concept of TS and may affect its policy implications.

[*] Corresponding author: dario.guarascio@uniroma 1.it

By exploiting network effects and winner-takes-all mechanisms, few digital corporations have acquired a systemic significance that existing regulatory frameworks have been unable to contain. Their economic size is now beyond that of large economies such as Germany or Japan; and their ability to influence government policy is unprecedented compared to that of multinational corporations in the past (Kenney and Zysman, 2020; Coveri et al., 2025a). This power ultimately stems from control over knowledge and critical infrastructures—such as data centers and submarine cables—and, most importantly, over 'dual-use' technologies, including cloud computing, AI, and advanced satellite navigation and communication systems that are vital to both civilian and military domains (Farrell and Newman, 2023; Coveri et al., 2025b). In this respect, Big Tech companies are now central actors in the confrontation between the two 'military-digital complexes' (Guarascio and Pianta, 2025)—the US and China—vying for global hegemony (Rolf and Schindler, 2023).

The growing power of Big Tech is the result of a long-term process characterised by the scaling back of the state's role in R&D activities (Archibugi and Filippetti, 2018), the emergence of "intellectual monopolies" whose development is closely tied to the privatisation of knowledge through patents (Pagano, 2014; Coveri et al., 2022), the privatisation of public goods and key infrastructures (Rikap, 2024), and the pervasive influence of the ICT sector in both the private and public spheres (Rikap and Lundvall, 2021). In the private sector, virtually all industries are increasingly dependent on the goods and services provided by large ICT companies, while in the public sector essential activities—from healthcare to defence—can hardly be pursued without relying on digital infrastructures and services controlled by Big Tech. Such a structural shift has been largely politically driven, rooted in the zero-cost transfer of technology from the public to the private domain and in the policy choices implemented in the United States during the 1990s, commonly referred to as the "commercialisation of the Internet" (Greenstein, 2000), which enabled a handful of companies to gain a first-mover advantage that ultimately led to the monopolisation of global digital markets, with the exception of China (O'Mara, 2020). During the most expansive phase of globalisation, neoliberal deregulation policies enabled these companies not only to secure dominant market positions, but also to gain control over key infrastructures abroad. Europe is emblematic in this regard, having developed a significant dependence on US Big Tech companies for the provision of most essential digital services (Draghi, 2024).

The progressive digitalisation of war reinforces Big Tech's influence by positioning major digital corporations at the core of military and intelligence activities (Coveri et al., 2025b). When critical capabilities and infrastructures are concentrated in the hands of few dominant firms, a government's capacity to exercise TS depends on its bargaining power vis-à-vis these corporations (Gjesvik, 2023). If the latter are in a position of strength, they can shape technological and infrastructural choices (i.e., orienting industrial policies towards specific products and eventually lock-in the government), influence international relations in line with their own interests (i.e., pushing for cooperative relations with regions in which their sales and investments are concentrated, and more confrontational ones with those hosting competitors or imposing hostile regulations), and, more broadly, promote actors and political positions aligned with their strategic objectives (e.g., preference for militarisation when arms-related digital services contribute to a significant share of their profits). At the same time, public spending (and particularly military procurement) plays an increasingly central role in Big Tech's profitability, while governments often act as crucial allies in shielding these firms from hostile measures adopted by foreign administrations, as illustrated by Trump's recent threats against the EU and Canada following fines imposed on US digital multinationals (Coveri et al., 2025b).

Therefore, even in countries that possess the financial, infrastructural, and technological resources required to pursue technological sovereignty (such as the US and China), the latter can be undermined when technological and geopolitical trajectories are steered in directions consistent with Big Tech's interests but at odds with its core objectives, including welfare (e.g., reducing market concentration, orienting R&D towards public health and environmental sustainability, limiting the privatisation of public assets and curbing inequalities) and cooperation (e.g., preserving international research, innovation and trade networks as well as institutions aimed at ensuring dialogue and cooperation among nation states) (Edler et al., 2023).

The relationship between military R&D and innovation in the commercial domain is also undergoing significant change (Guarascio and Pianta, 2025). In the past, many radical innovations originated in the military sphere and subsequently spilled over into the commercial sector, as in the case of the Internet (Mowery, 2010). Today, however, the pervasive digitalisation of goods and production processes—including within the military—has partly reversed this dynamic. Transformative digital applications are now largely developed in the civilian domain, and the dominant Big Tech firms that are best positioned to identify, adapt, and transfer these innovations to the military at scale. This shift grants additional leverage to these corporations and helps explain both the 'revolving door' between Big Tech and the military (Coveri et al., 2025a) as well as the creation of dedicated institutions such as the Defence Innovation Unit, based in Silicon Valley, which seeks to channel digital innovation into the defence sector (Harper, 2020). It also contributes to the relative downsizing of traditional defence contractors, which have themselves become increasingly dependent on Big Tech for digital services and components that are now indispensable on the battlefield (as vehicles and arms becomes digital, purchasers, including the Department of Defense, become dependent on suppliers for continuous software updates and maintenance).

In one of the key areas of TS—security—the mutual dependence between the state and Big Tech can weaken public control over defence-related R&D and bias decision-making, favouring technological lock-in and, hence, maximising the rents extracted by digital companies. Equally significant is the private control over infrastructure that stores and processes sensitive and classified data, paving the way for a form of 'privatised technological sovereignty' in which private interests can exert substantial influence over industrial and security policy decisions (Abels, 2026).

Outside the US or China, the dependence on Big Tech has increased substantially in the recent past: extensive reliance on their cloud and AI-related services implied a loss of control over infrastructures and technologies that are essential to R&D, innovation, and the functioning of large parts of the economy (Rikap, 2024); the transfer of substantial shares of value added abroad—whose accumulation is facilitated by tax avoidance; and pervasive surveillance and data extraction, with significant implications for competition, security, and international relations. Power asymmetries are further reinforced by the fact that Big Tech firms are not merely suppliers of essential technologies and services; they also function as the 'eyes and ears' of their military–digital complexes, absorbing (and, if required, transferring to their government) intelligence-relevant information and participating directly in contemporary conflicts (e.g., Gaza, Ukraine). Building on such a peculiar role, Big Tech strengthen their market positions and affect the decisions of the governments they interact with on crucial matters such as digital and defence-related procurement and infrastructures (Gonzalez, 2023).

In this context, the very concept of TS requires a critical reassessment, paving the way for a series of highly significant research questions. To what extent does the polarisation of the global economy, shaped by the State–Big Tech nexus in the United States and China, calls into question the actual possibility of achieving TS? Is it possible to shape technological and infrastructural development, and to ensure sustainable economic growth, under conditions of radical technological dependence? Is TS achievable when network infrastructure, AI or satellite systems are wholly or largely controlled by private corporations? How is this challenge compounded when those corporations are foreign? Relatedly, could we develop a "typology" of TS that, by referring to different structural and governance frameworks, highlights variations in both the relative weight of the private sector and the capacity of states to pursue TS? What position does Europe occupy within this complex web of economic, technological and geopolitical power relations?

This work aims at answering to these research questions, contributing to the growing literature on TS (Edler et al., 2023). First, we empirically examine the long-term trends shaping the current configuration of economic and technological power: the growing influence of the private sector in R&D activities, the increasing centrality of digital technologies within sectoral and technological hierarchies, the emergence of US and Chinese Big Tech firms and their dominance over knowledge, infrastructures, and key technologies such as cloud computing and AI; as well as the deepening technological and infrastructural dependence of the European economy (Section 2). Second, building on (Coveri et al., 2025a), we analyse the growing

mutual dependence between Big Tech and the military apparatus, showing how it reinforces the economic power of the private actors involved, weakens the state's capacity to act autonomously, and intensifies the subordination of foreign governments dependent on US and Chinese digital platforms (Section 3). Third, we propose and discuss a typology of TS that takes into account the degree of technological dependence on Big Tech, the nature of the relationship between states and digital companies, and, consequently, the state's capacity to align the activities of these companies with its own strategic objectives (Section 4). The final section concludes with a discussion of the policy implications (Section 5).

2. Privatisation of R&D, intellectual monopolies and the rise of Big Tech

Privatisation of R&D and the consolidation of intellectual monopolies

The technological hegemony of the state during the Cold War was predicated on its role as a primary risk-taker. General-purpose technologies—such as the Internet, GPS, and early microelectronics—were driven by mission-oriented public R&D, heavily subsidized and directed by the military-industrial complex (Mowery, 2009). In this paradigm, radical innovations originated in the public sector before being adapted to civilian and commercial uses. During the post-1945 period, public spending (notably in defence-related areas and in biomedical research) has been a fundamental force shaping the industrial R&D system, particularly in the US. Although the approach and scale differed —notably because the military sector played a less prominent role— a similar pattern can be observed in other advanced economies, including major European economies, Japan and South Korea, where the state acted as a crucial peacetime actor in the "national innovation system", especially through direct R&D funding. At this stage, the state's ability to steer the course of technological development is significant, basic research plays a key role, and competition policy makes it possible to promote innovation while containing market concentration (Mowery and Nelson, 1999).

Focusing on the US, Mowery (2009) shows how federal R&D spending accounted for more than 50% of total national R&D spending during 1953–1978 and dropped below 40% only in 1991, reaching its postwar low point of 25% in 2000. In this context, defence-related R&D investment played a key role: in the late 1950s and early 1960s, it accounted for one-half of total national R&D spending. However, structural changes that followed began to alter the nature of the innovation system—both within and outside the United States—leading to a gradual reduction in the role of the state in favour of the private sector and, consequently, to a concentration of economic and technological power largely driven by the privatisation of knowledge, with intellectual property protection and market deregulation policies playing a central role (Pagano, 2026).

In the US, this shift was reflected in a series of institutional and regulatory changes. Antitrust restrictions on research collaboration were reduced, enforcement of intellectual property protection was improved (e.g., the Bayh-Dole Act of 1980 simplifying federal policy toward intellectual property resulting from federally funded R&D)[1], review procedures for mergers were relaxed while major federal antitrust suits against high-technology firms were dropped or settled in the early 1980s (e.g., the 1984 National Cooperative Research Act (NCRA) reduced the antitrust penalties for collaboration among firms in precommercial research[2]). Equally important, patentability has been extended to previously excluded fields such as software, business methods, and biological inventions. At the same time, patent standards have been significantly relaxed, blurring the boundary between pure information and practically applicable knowledge, contributing to the

[1] The Act promoted university patenting and licensing by establishing a uniform policy to replace previous agreements between universities and federal agencies, endorsing exclusive licensing arrangements with industry for federally funded research, and reducing federal oversight of licensing terms for patents arising from such research. Moreover, the establishment of the Court of Appeals for the Federal Circuit (CAFC) further strengthened the protection granted to patentholders. As the court of appeal for patent cases throughout the federal judiciary, the CAFC soon emerged as a strong champion of patentholder rights.

[2] The NCRA has been credited with facilitating the early growth and operation of the Microelectronics and Computer Technology Corporation, a research consortium involving US computer and electronics firms.

‘upstreaming’ of patentability—the tendency for intellectual property rights to extend increasingly close to abstract ideas (Pagano, 2014).

At the international level, a series of institutional discontinuities opened the way for large multinational firms to own ‘a disproportionate share of the global knowledge’: the 1994 Marrakesh (TRIPS) agreements, following the establishment of the World Trade Organization, allowed the (few) companies with the necessary financial and technological capabilities to enjoy the fruits of past public investment in knowledge accumulation as well as the incentives of knowledge privatisation. The fast diffusion of ICTs, to a large extent stemming from earlier publicly funded R&D, further strengthened this process stimulating private investments attracted by the possibility to secure intellectual property rights (Pagano and Rossi, 2009).

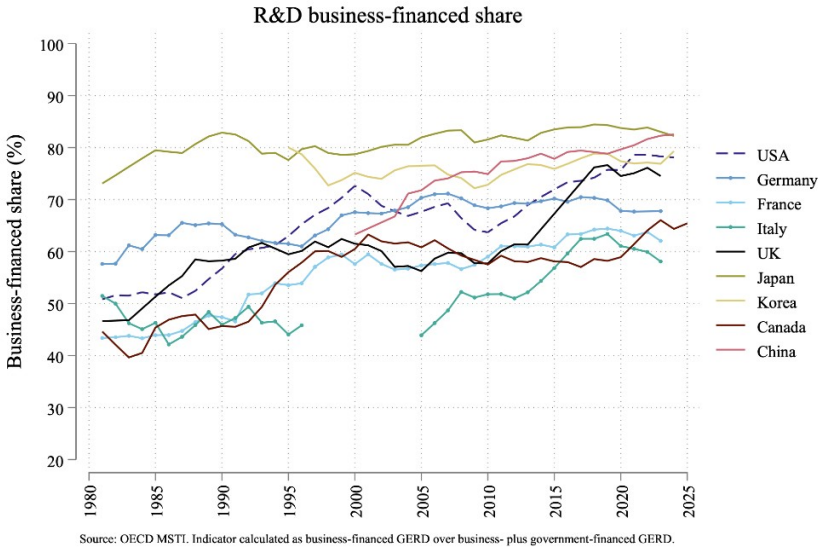
Another major discontinuity regards the gradual reduction in military-related R&D spending during the early stages of globalisation, partly as a consequence of the end of the Cold War and partly as part of a broader restructuring of the US innovation system aimed at raising productivity growth and responding to the fierce competition in manufacturing. After reaching its peak (nearly 70% of total Federal R&D in 1987), the defence-related share of R&D spending began a decline (a topical moment is the ‘last supper’, a historic 1993 dinner meeting where then-Defence Secretary Les Aspin told CEOs of the US largest defence contractors that post-Cold War budget cuts were coming), reaching a low point of 54% in 1999, to then restart growing in response to the 11 September 2001 attack.

There are therefore four key processes reshaping the functioning of the US and global economy, as well as the relationship between the state and private capital in the generation and exploitation of knowledge: a reduction in the state’s role in knowledge production and a partial scaling back of military R&D; the privatisation and expansion of multinational corporations benefiting significantly from the new regimes of deregulation and intellectual property rights; and the rise of the ICT sector as a major attractor of investment in R&D and innovation. What are the consequences? The US start asserting technological leadership supported by the new regime of knowledge privatisation while techno-economic power becomes concentrated in a small number of large multinational corporations contributing to the rise in inequalities and economic polarisation; alongside a parallel decline in the role of the state and of basic and open research (Mazzucato, 2013).

Figure 1 documents what Archibugi and Filippetti (2018) call the “retreat of public research”, a process that —although more pronounced in the United States—has characterised virtually all advanced economies since the early 1980s (note that Chinese figures are likely biased, as OECD data do not distinguish between private and state-owned enterprises). The share of business-funded R&D in total has grown steadily between 1980 and 2025, with the sharpest increases observed in the US (from about 50% in the 1980s to close to 80% in 2025) and in the UK (from 47% to about 76%). While following the same general trend, other European economies have experienced a somewhat slower rise in the private share of R&D, highlighting structural heterogeneity across national innovation systems.

Figure 1. The retreat of public R&D – share of business-financed R&D over total R&D expenditure

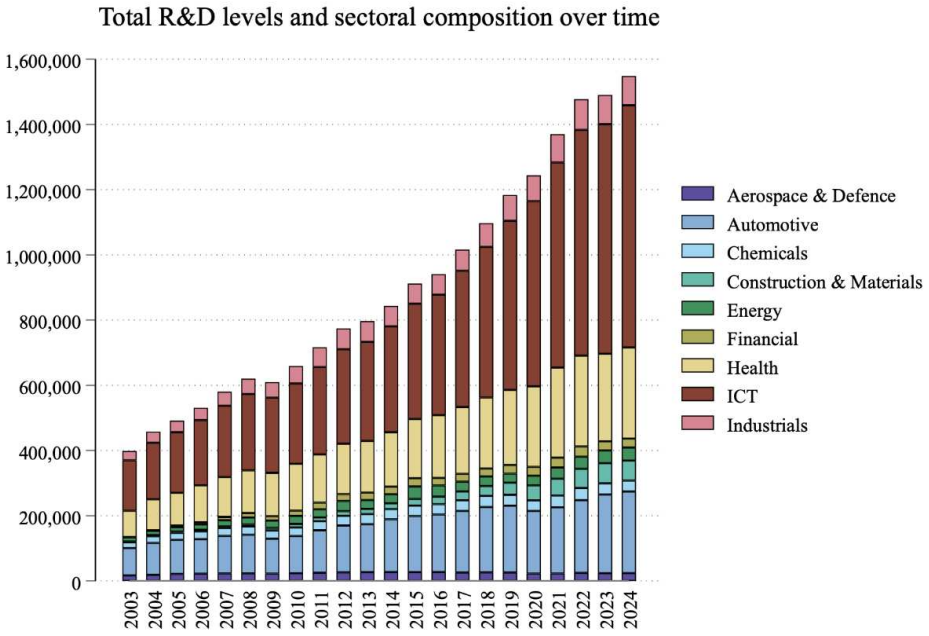
(selection of OECD countries and China – 1980-2025)



Source: Authors' elaboration on OECD data

Such dynamics goes hand in hand with another major structural shift: the growing importance of the ICT sector—driven initially by the diffusion of personal computers, the emergence of the Internet and the network economy, and later consolidated through smartphones, the Internet of Things, and global connectivity—has profoundly reshaped production, consumption, markets, and technological and research dynamics. Figure 2 illustrates how, between the early 2000s and 2024, the ICT sector became increasingly central to knowledge creation; while Figure 3 shows how top ICT firms are increasing the share of global R&D expenditure under their control.

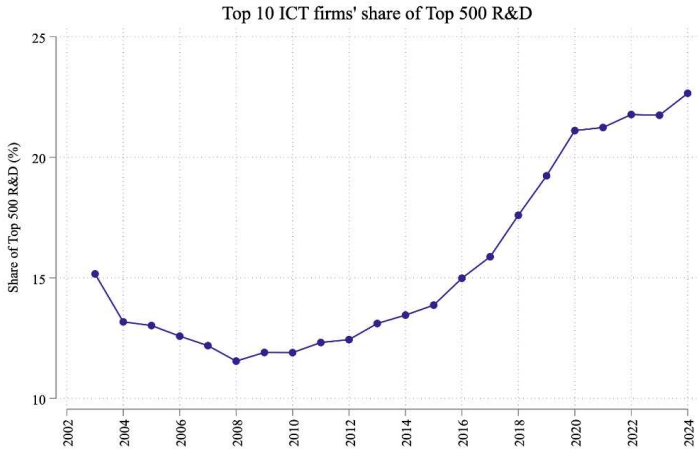
Figure 2. Total R&D investments (US$ million, PPP) and sectoral composition over time (2003-2024)



Source: Authors' elaboration on OECD data

These trends are closely linked to the rapid consolidation of intellectual monopolies—most of which are concentrated in the ICT sector—which are capturing an increasing share of globally generated knowledge and value added. The archetype is the large digital platforms or Big Tech—initially US-based, with Chinese platforms emerging later—which, by controlling the knowledge, data, and infrastructure required to store and process them, are able to exploit economies of scale and network effects more effectively than ever before, thereby acquiring unprecedented tech-economic power (Coveri et al., 2022). As documented by Rikap (2024), these corporations capture and enclose global knowledge networks through aggressive patenting strategies, the monopolization of massive proprietary datasets, and the continuous poaching of top-tier academic talent from public universities. Rather than simply selling products, these corporations monopolise the intangible assets and methods necessary to produce further innovation (Durand and Milberg, 2020). For the state, the consequence is profound: it is no longer just buying technology; it is operating within proprietary ecosystems where the rules, standards, and protocols are dictated by corporate entities.

Figure 3. Top 10 ICT firms's share of top 500 R&D (2002-2024)



Source: authors' elaboration on OECD data.

This creates an insurmountable barrier to entry, preventing public institutions from organically rebuilding the capabilities they abandoned during the retreat of public research. Empirically, such developments could be visualised in different ways.

Table 1. Top 20 R&D spenders by sector and country (2003)

R&D (US$ million, PPP) and share over total top 2000 R&D spenders

Ranking top 20, 2003

Company	Sector	Country	R&D	Share (%)
MICROSOFT	ICT software	US	10.107,61	2,35%
FORD MOTOR	Automotive	US	9.745,10	2,27%
PFIZER	Health	US	9.265,64	2,16%
MERCEDES-BENZ	Automotive	Germany	9.105,33	2,12%
SIEMENS	ICT hardware	Germany	9.007,27	2,10%
GENERAL MOTORS	Automotive	US	7.406,27	1,72%

VOLKSWAGEN	Automotive	Germany	6.766,48	1,57%
IBM	ICT software	US	6.585,09	1,53%
TOYOTA MOTOR	Automotive	Japan	6.287,82	1,46%
SANOFI	Health	France	6.274,60	1,46%
JOHNSON & JOHNSON	Health	US	6.086,13	1,42%
GSK	Health	UK	5.880,45	1,37%
NOKIA	ICT hardware	Finland	5.768,69	1,34%
INTEL	ICT hardware	US	5.665,15	1,32%
PANASONIC	Others	Japan	5.338,13	1,24%
MOTOROLA	ICT hardware	US	5.289,19	1,23%
SAMSUNG ELECTRONICS	ICT hardware	South Korea	5.247,45	1,22%
SONY	Others	Japan	4.972,07	1,16%
ASTRAZENECA	Health	UK	4.757,30	1,11%
HP	ICT hardware	US	4.745,21	1,10%

Source: Authors' elaboration on JRC R&D scoreboard data

First, displaying the growing dominance of a small group of ICT corporations among the top private R&D spenders as reported in Figure 3: after a slight decline between 2002 and 2008, their share starts increasing exponentially reaching about the 23% of the total expenditure incurred by the top 500. Second, examining the significant shift in sectoral and geographical rankings since the early 2000s: a comparison of the top 20 R&D spenders in 2003 and 2024 reveals several important changes (Tables 1 and 2). While in 2003 eight of the ten companies were ICT firms, by 2024 this number rises to eleven, with ICT firms occupying the top seven positions. The European presence declines significantly, with only two German automotive firms remaining in the ranking; Japan maintains its (modest) position, and, most notably, a clear concentration (and polarisation) of power in US and China emerges.

Table 2. Top 20 R&D spenders by sector and country (2024)

R&D (US $, PPP) and share over total 500 top R&D spenders

Ranking top 20, 2024

Company	**Sector**	**Country**	**R&D**	**Share (%)**
AMAZON	ICT software	US	54.187,61	3,26%
HUAWEI	ICT hardware	China	43.728,52	2,63%
ALPHABET	ICT software	US	38.270,37	2,30%
META	ICT software	US	34.831,10	2,10%
SAMSUNG ELECTRONICS	ICT hardware	South Korea	34.366,43	2,07%
MICROSOFT	ICT software	US	25.942,66	1,56%
APPLE	ICT hardware	US	25.049,90	1,51%
VOLKSWAGEN	Automotive	Germany	22.614,36	1,36%
TENCENT	ICT software	China	17.767,40	1,07%
ALIBABA GROUP HOLDING	ICT software	China	14.365,28	0,86%
JOHNSON & JOHNSON	Health	US	13.760,28	0,83%
INTEL	ICT hardware	US	13.212,48	0,80%
BYD	Automotive	China	12.720,92	0,77%
MERCK US	Health	US	12.123,29	0,73%
TOYOTA MOTOR	Automotive	Japan	11.953,92	0,72%
CHINA ST CONST. ENG.	Construction & Materials	China	11.416,57	0,69%

HONDA MOTOR	Automotive	Japan	10.909,68	0,66%
MERCEDES-BENZ	Automotive	Germany	10.444,52	0,63%
NVIDIA	ICT hardware	US	10.312,22	0,62%
ASTRAZENECA	Health	UK	10.074,55	0,61%

Source: Authors' elaboration on JRC scoreboard data

Contrary to its initial promise that economic and innovation opportunities would spread globally and more evenly, the expansion of the internet has instead contributed significantly to the concentration of power in the hands of a small number of digital platforms also known as Big Tech (O'Mara, 2020; Coveri et al., 2022). Platform business models rely on the accumulation and control of vast flows of personal, behavioural, and economic data generated through the networks they operate (Zuboff, 2019). This creates a highly asymmetrical distribution of information that undermines the conditions required for effective market competition and increase their ability to capitalise on network effects (Calvano and Polo, 2021) and winner-takes-all mechanisms (Gawer, 2022). In addition, platforms' cross-sectoral reach and their use of cross-subsidisation and selective below-marginal-cost pricing strategies complicate conventional tools for assessing and contrasting excessive market power (Kenney and Zysman, 2016). By connecting as many applications as possible to the dominant platform, they have managed to extend their reach and lock-in users, complementors and competitors making technological competition a means to an end rather than a threat to their market power (Gawer and Cusumano, 2014; Jacobides et al., 2024). In the relationships with other firms, digital platforms are able to offer unique channels for specific business services, data management, marketing, logistics, delivery; they can extract rents from companies that are ever more dependent on their services (Cutolo and Kenney, 2021).

In addition to their monopolistic control over key infrastructure (such as submarine cables, datacentres and cloud services) and technologies (Gjesvik, 2023), Big Tech firms derive further power from their peculiar ability to influence the state. Beyond using a share of their substantial profits for traditional lobbying, these companies can leverage their control over digital spaces (i.e., social media) where a growing share of information and political consensus is formed, as well as their capacity to mobilise a highly locked-in customer base, to resist regulatory pressures including measures aimed at limiting personal data appropriation, increasing taxation or curbing their scope of activity (Culpepper and Thelen, 2020). This results in an unprecedented concentration of economic power. Focusing on US Big Tech—analogous platform firms such as Alibaba or Tencent have emerged in China over the past two to three decades—Table 3 highlights the scale of this power by examining market capitalisation, revenues and operating income.

Table 3. Alphabet, Amazon, Apple, Meta and Microsoft
Market capitalization, revenues, operating income and employees

	Market capitalisation June 2026 (USD, trillion)	Revenues 2025 (USD, billion)	Operating Income 2025 (% of revenues)	Employees 2025
Alphabet	4,33	403	32%	190.820
Apple	4,28	416	32%	166.000
Microsoft	2,95	282	46%	228.000
Amazon	2,56	717	11%	1.576.000
Meta	1,45	201	41%	78.865
Total	15,57	2019	27%	2.239.685

Source: Authors' elaboration on Yahoo Finance data (accessed June 11, 2026)

Such a concentration of economic power challenges standard theories of the firm, which are grounded in assumptions of competition and the eventual subordination of firms to state regulation (for a thorough discussion of this point, see the special issue of the Cambridge Journal of Economics 'Big Tech Oligopolies,

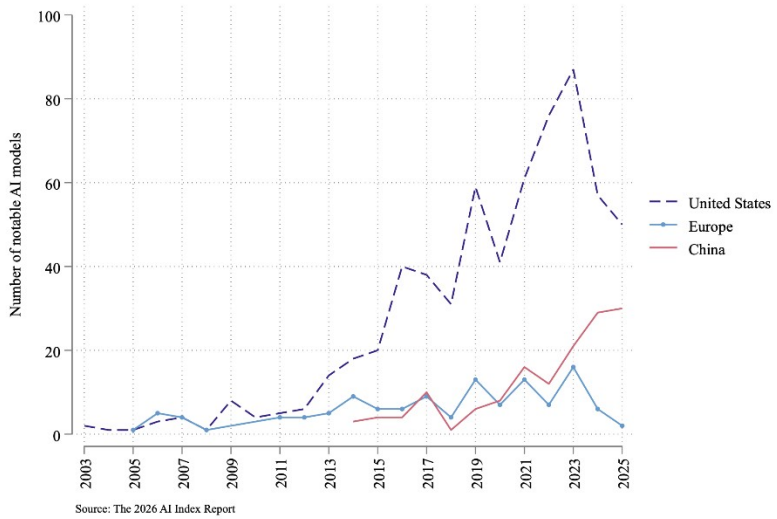
Keith Cowling, and Monopoly Capitalism', Conyon et al., 2022). Big Tech's capacity to weaponise assets, technologies, and proprietary knowledge can significantly constrain the public sector's ability to regulate markets, pursue industrial policies, and shape technological trajectories, thereby calling into question the very notion of TS. By contrast, employment figures point to another distinctive feature of Big Tech: these firms are able to excert extraordinary economic power with a comparatively limited workforce. The concentration of market value, revenues and profits is therefore only weakly reflected in employment data, with Amazon representing the main exception because of its labour-intensive logistics, warehousing and delivery activities.

Infrastructures, frontier technologies and the growing dominance of Big Tech

The global and cross-sectoral power of Big Tech has expanded alongside the digitalisation of the world economy. The growing centrality of digital markets, together with the indispensability of cloud services, platforms, and connectivity infrastructures, has reinforced the dominance of the largely private actors that control these technologies. At the same time, Big Tech firms dominate digital innovation ecosystems and continue to accumulate highly idiosyncratic capabilities, making their technological advantages increasingly exclusive and difficult to challenge (Guarascio and Pianta, 2025).

The diffusion of machine learning and, more recently, neural network-based AI has further strengthened this position. These technologies function both as general-purpose technologies—enabling innovation across the economy—and as a new method of invention (Bianchini et al., 2022; Arenas Diaz et al., 2025), granting substantial power to those who control the underlying knowledge base, AI models, and the infrastructure and computing capacity required for their operation, particularly data centres (Fanti et al., 2022). Unsurprisingly, these strategic assets are concentrated largely in the hands of US and Chinese Big Tech firms, which consequently play a leading role in shaping public debates and policy strategies surrounding AI regulation.

Figure 4. Number of notable AI models

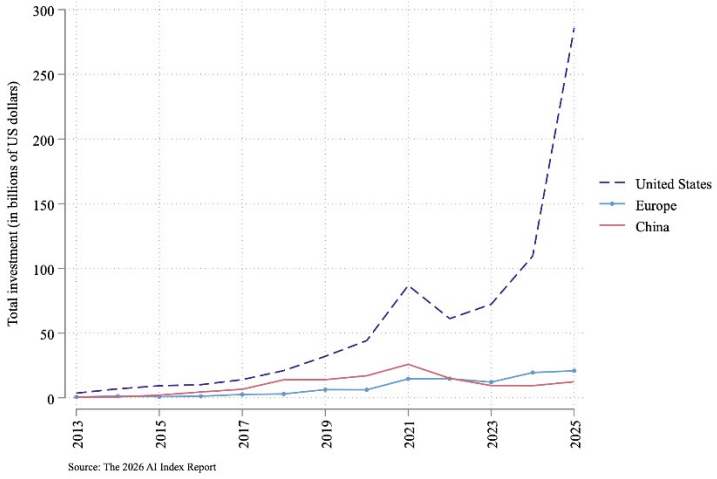


Source: Authors' elaboration on Stanford HAI Report data.

Their dominant position is further reinforced by the remarkably fast diffusion of AI—GenAI reached 53% adoption in three years, faster than the personal computer or the Internet—and by its capacity to intensify the surveillance-based tools and mechanisms through which major platforms have already secured control over large segments of the global economy. This is not the only consequence of the spread of AI, though. Given the local and idiosyncratic nature of knowledge and innovation as well as the key role of innovation systems in shaping technological capabilities and competitiveness, it is unsurprising that technological leadership in

this field is increasingly contested between the United States and China, while much of the rest of the world risks falling into a position of growing technological dependence.

Figure 5. Private investments in AI (billions of US dollars)



Source: Authors' elaboration on Stanford HAI Report data.

Figure 4 shows the distribution of notable AI models—that is, models achieving state-of-the-art results on recognised industry benchmarks—between 2003 and 2025. The United States appears to be ahead of both China and Europe, with 50 models in 2025, compared to 30 in China and only 2 in Europe. Although this information is useful for understanding geographical polarisation, the distribution of models alone is insufficient to fully assess the position of different actors, since performance and market penetration are equally—if not more—important.

What can nevertheless be identified is the relative influence of state and private actors within the AI-related technology and knowledge sectors, as well as the differing industrial policy strategies shaping the development of this technology, particularly with regard to the relationship between states and corporations. Analysing the evolution of private investments in AI technologies (Figure 5), the US stands out again as the leading player. However, when it comes to AI-related public spending the picture changes radically. While the divide between the United States and Europe remains stark, China's position stands out in a clear-cut way. Between 2003 and 2024, cumulative public spending on AI in the United States—including grants, contracts, and Other Transaction Agreements (OTAs)—rose substantially, from $0.08 billion to $20.5 billion. Over the same period, however, China's central and local government venture capital funds channelled an estimated $912 billion into strategic industries related to AI, drawing on tax revenues, land-sale proceeds, and contributions from state-owned partners.[3]

Table 4. Top patent owners in GenAI

Number of patents (2014-2023)

Company	Country	# of patents (~)
Tencent	China	2200
Ping An Insurance Group	China	1500
Baidu	China	1300
Chinese Academy of Science	China	610
IBM	US	600
Alibaba	China	580
Samsung	South Korea	450
Alphabet	US	440
Bytedance	China	420

[3] Source: Stanford HAI Report.

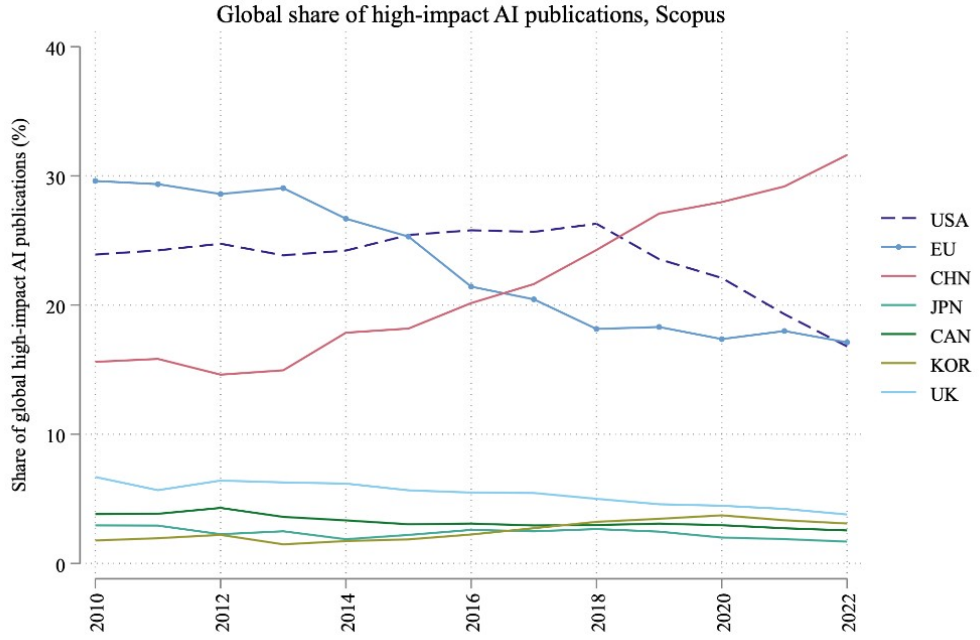
Microsoft	US	390

Source: Authors' elaboration on WIPO data

According to Beraja et al. (2024), a majority of Chinese AI firms (71%) that received both government and private venture capital funding obtained government investment first, which then served as a signal encouraging private VC investment. The global AI hierarchy thus follows a distinctive pattern: the United States and China are competing for dominance in the sector, while Europe remains in a clearly subordinate position. While in the US case, this competition is driven largely by the private sector, which accounts for most investment, in China the government plays the leading role, both by financing investment and by intervening directly in the industry through state-owned enterprises.

Power is even more concentrated concerning AI-related knowledge. Table 4 reports the top ten patent owners considering patent families related to GenAI. China and the United States clearly dominate the sector; indeed, only one company among the top ten does not belong to either of these two blocs, namely South Korea's Samsung. Nevertheless, China appears to have gained a substantial advantage, with six of the ten entities included in the ranking. Here too, however, the distinctive characteristics of the two national innovation systems and industrial policy strategies are clearly evident with the public sector playing a prominent role in China as opposed to the US. The Chinese Academy of Sciences alone holds more GenAI-related patents than major players in the US digital ecosystem such as Alphabet, IBM, and Microsoft. Moreover, among the leading patenting universities and research organisations, nine out of the top ten are Chinese. The top three positions are occupied by the Chinese Academy of Sciences, Tsinghua University, and Zhejiang University, while the first US institution to appear in the ranking is the University of California, in tenth place.[4]

Figure 6. Global share of high-impact AI-related scientific publications (2010-2022)



Source: Authors' elaboration based on OECD data

China also appears to hold a leading position in high-impact AI-related scientific publications (Figure 6). Having started in 2010 well behind both the United States and Europe, China now accounts for more than 30% of total high-impact AI-related publications, while the other two regions remain below 20%. These figures highlight the substantial effort undertaken by both the Chinese government and the domestic private

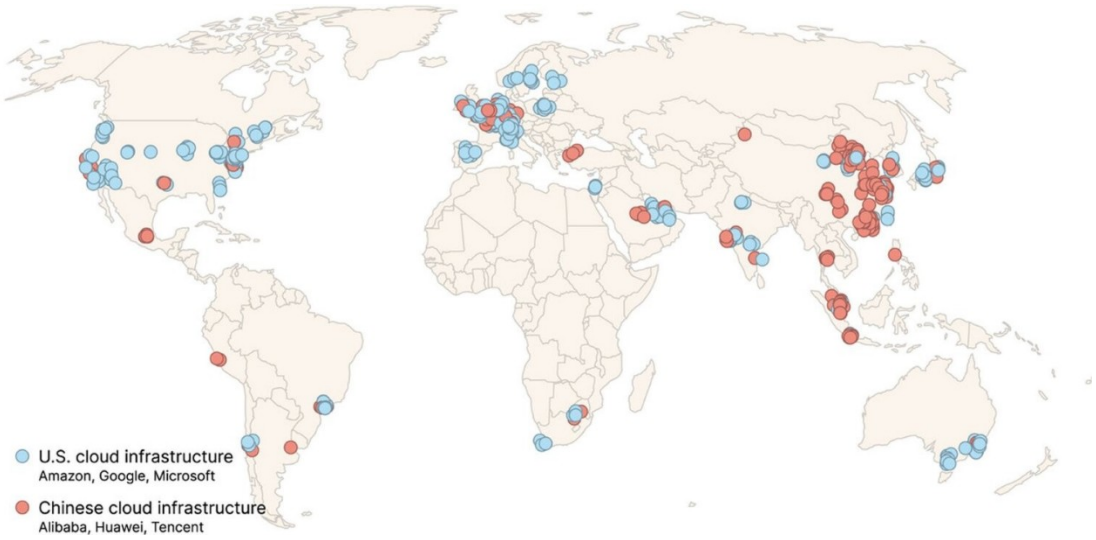
[4] Source: WIPO.

sector to win the ‘AI race’, reflecting the perception that leadership in AI is crucial for achieving economic, technological, and geopolitical dominance (Sun and Kenney, 2025).

Lehdonvirta et al. (2025) have documented how US and Chinese Big Tech corporations holds virtually all the world economy in a condition of techno-infrastructural dependence by controlling the large majority of the data centers on which the operation of the global digital network is based. These authors analyse the so-called Availability Zones (AZs) intended as ‘interconnected data centres together with the associated power, cooling, and networking infrastructure’. The latter are now by and large controlled by Big Tech providing connectivity, cloud and AI-related services in a given country.[5]

The geography of AZs is striking (Figure 7): US and Chinese Big Tech effectively split the global market among themselves, controlling the supply of connectivity, computing power, and related services; drawing on an almost inexhaustible flow of data that improves the performance of algorithms and dual-use technologies; and reinforcing their systemic and infrastructural position relative to both private and public actors.

Figure 7. Geographical distribution and ownership of datacenter/cloud availability zones (2023)

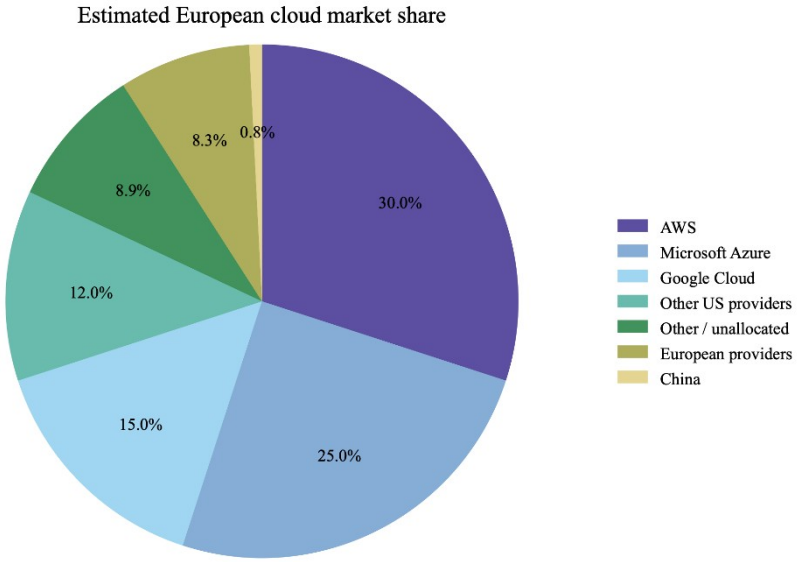


Source: Lehdonvirta et al. (2025)

As documented, the combined annual R&D budgets of Big Tech now vastly eclipse the total public R&D budgets of nation states, major national science foundations and European framework programs. This financial asymmetry transforms the relationship between the state and capital from one of procurement to one of a ‘tenant and landlord’ (Coveri et al., 2022, 2025a). In addition, there is a growing dependence on the infrastructure that underpins the digital services provided by Big Tech, such as AZs. This is what Albels (2026) frames as ‘privatised technological sovereignity’. Given the local, cumulative, and path-dependent nature of the underlying technological and infrastructural knowledge and capabilities, this dependence tends to intensify over time. From this perspective, the European case is particularly revealing.

Figure 8. Estimated European cloud market share by provider (2025)

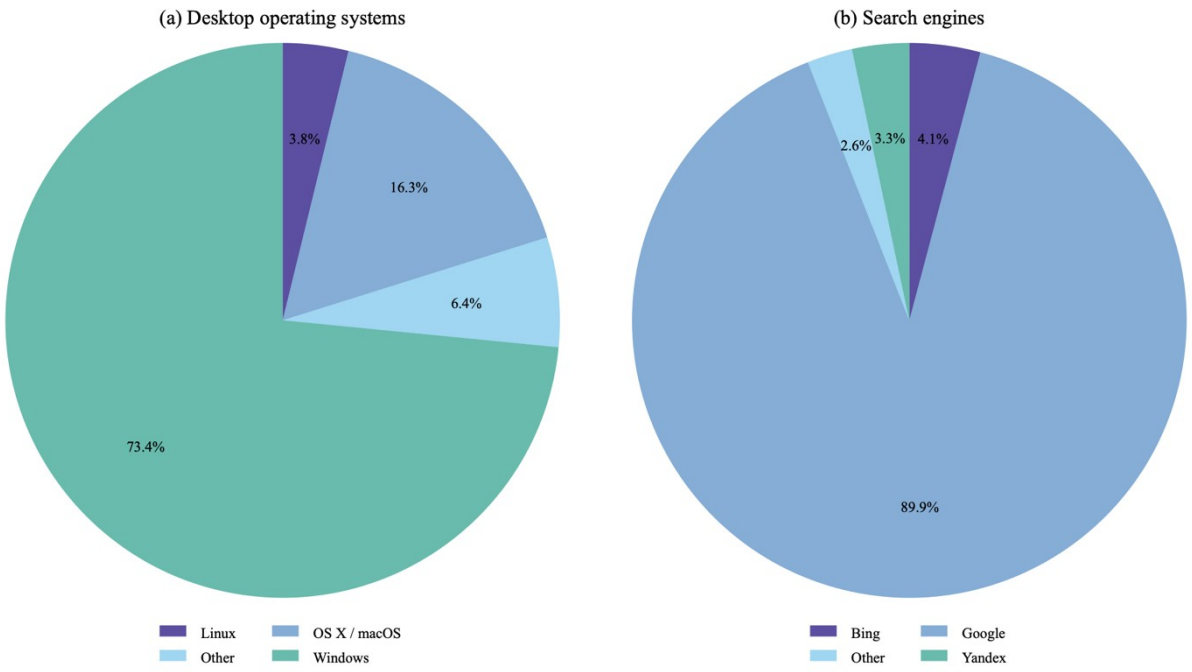
[5] The authors conducted a census of all AZs operated by the top three US and top three Chinese global providers (Amazon Web Services, Microsoft Azure, Google Cloud, Alibaba Cloud, Huawei Cloud, and Tencent Cloud) as of October 2023 relying on publicly available sources, including cloud providers’ websites and customer-facing interfaces. These providers were. As Lehdonvirta et al. (2025) emphasise, Big Tech also rely on a number of smaller facilities, including various forms of edge computing infrastructure. However, AZs account for the majority of data storage and processing activities.



Source: Authors' elaboration based on Gineikyte-Kanclere, V. et al. (2025), Annex 3

In Europe, more than the 80% of the cloud services are provided by US-based corporations. The latter include: AWS (30%), Microsoft (25%) and Google cloud (15%) followed by other US (12%), Chinese (0.8%) and European (8.3%) providers (Figure 8). This is a striking piece of evidence: the vast majority of everyday activities carried out by European citizens, businesses, and public administrations depend on a small number of entities whose power can shape the economic fortunes of individual actors, the balance of power between states and corporations, and broader geopolitical dynamics. A very similar picture emerges when looking at the European software market (operating system and search engines) in Figure 9.

Figure 9. Operating systems and search engines in Europe (market shares in 2025)



Source: Authors' elaboration based on Gineikyte-Kanclere, V. et al. (2025)

In the operating system market, concentration is the result of a long-term process that started developing in the 1990s: Microsoft holds more than 75% of the European market (a slight decline from nearly 85% in 2015), followed at a considerable distance by another US Big Tech firm, Apple. There is even more concentration in the search engine market, where Alphabet/Google controls almost 90% of the market. European weakness extends further to the 'hardware' through which digital technologies enter everyday life: smartphones, tablets and laptops. The EU market is flooded by foreign producers—Apple, Samsung, Xiaomi and Huawei, among others—with no EU corporation capable of producing smartphones or laptops at scale (Guarascio and Pianta, 2025). What matters here is not only the welfare implications of such concentration (albeit highly significant), but a deep, multi-layered dependency spanning knowledge, technology, infrastructure, and critical services, which places Europe in a position of subordination and may ultimately undermine its ambitions for TS. As will be shown in the next Section, the situation is even more complex, as the integration of Big Tech companies with government and military structures further amplifies their power in practice, while also making their relationships more problematic in geopolitical terms and constraining the ability of governments outside the United States and China to implement effective industrial and innovation policies.

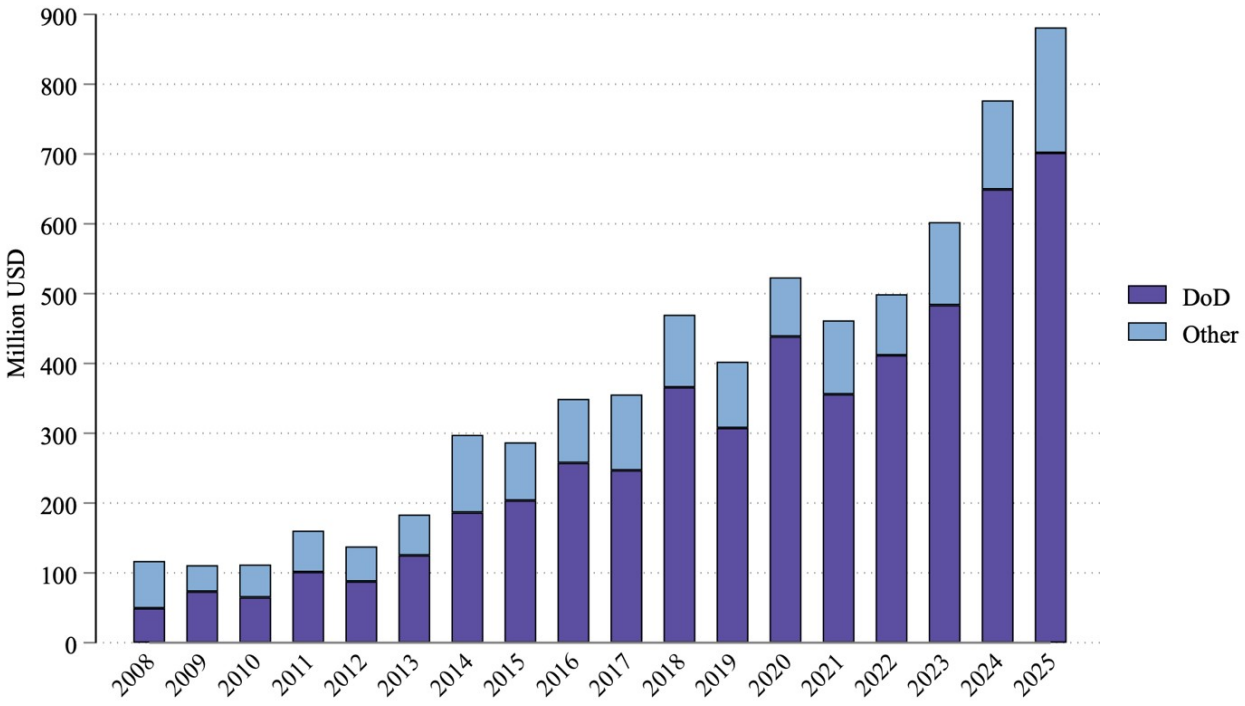
3. The military-digital complex

Big Tech firms and their government are bounded by a relationship of mutual dependency (Coveri et al., 2025a). The government cannot do without knowledge, technology and infrastructures held by large digital platforms. By the same token, these companies play a pivotal role in the functioning of the broader economy by providing essential digital services. They manage platforms that are central to the dissemination of information and the formation of public opinion and, much like—if not more than—the multinational corporations of the twentieth century, they possess significant tools of political influence, such as lobbying, which help shield them from unfavourable state intervention and regulation (Rahman and Thelen, 2019).

At the same time, Big Tech remains deeply dependent on the state. Governments regulate and provide the infrastructure and public goods—such as education and universities—necessary for the functioning of markets and of Big Tech itself. They support these firms in accessing and expanding within international markets and often intervene on their behalf in disputes with foreign governments, as illustrated by recent tensions in which the Trump administration openly defended US digital firms against EU and Canadian regulatory initiatives. Moreover, by deregulating markets or refraining from imposing restrictions—for example, through federal efforts to block stricter AI regulations introduced by US states—governments enable these firms to pursue objectives crucial to their business models, including access to personal and sensitive data. Public authorities also increasingly delegate the management of essential services to these corporations, allowing them to extract substantial profits (and data) from activities of systemic importance (e.g., health, education).

Although the United States and China differ significantly in terms of the role of the state and its relationship with markets and firms, both systems are characterised by a strong mutual dependence between the state and Big Tech. In both cases, this interdependence is further reinforced by the growing integration of major technology firms with military and intelligence structures—what Guarascio and Pianta (2025) describe as the 'military-digital complex'.

Figure 10. US Federal procurement contracts
awarded to Alphabet, Amazon, Meta and Microsoft, 2008-2025



Source: Adaptation from Coveri et al. (2025b) based on the US spending data;
Notes: DoD refers to the Department of Defence

While the activities of US digital corporations have largely developed in commercial domains, some characteristics of their technologies have made them relevant for warfare and intelligence activities too. The digitalisation of warfare—where the effectiveness of military and intelligence operations increasingly depends on technologies such as AI, autonomous weapons, cyberwarfare systems, and automated decision-support tools—has made Big Tech's expertise, infrastructure, and technological capabilities essential to the pursuit of strategic and military objectives. This dynamic further consolidates the relationship between governments and digital platforms, adding a security, military, and geopolitical dimension to the power of Big Tech while increasingly blurring the boundaries between the state and private capital.

Figure 10 illustrates the continuous growth of procurement contracts awarded between 2008 and 2025 by US Federal agencies to Big Tech, to a large extent stemming from the Pentagon (similar dynamics taking place in China have been recently documented by Guarascio, 2026). Although the monetary value of these contracts is tiny compared to Big Tech's revenues from commercial markets, the figure is most likely underestimated. Two are the main reasons. First, a large number of multiannual defence-related procurement contracts are classified or not available in publicly available data sources (Gonzales, 2022). Second, Big Tech provide key digital technologies and services to traditional defence procurers (e.g., Raytheon, RTX) thereby generating profits that are indirectly tied to military spending. The figure is also conservative because it focuses only on four Big Tech firms. Adding Palantir would double the value of the procurement flows in Figure, given its strategic position not only in defence and intelligence infrastructures (through Gotham and Maven-related systems)[6] but also in domestic security, including ICE case-management systems.

Table 5. Selected US Military contracts to Big Tech companies, 2013-2026

Year and Dept.	Contractor	Amount in USD	Nature of activities	Stated objective
2013 – CIA	Amazon	600 million	Cloud	Data management for preventing terrorist attacks

[6] As illustrated by two recent Maven-related Army contracts alone, worth almost 600 million USD.

2017 – DoD / DISA	Microsoft	58,3 million	Consulting and technical support	Microsoft Enterprise Technical Support Services for the F-35 Joint Program Office.
2019 – DoD; Project Maven	Alphabet (withdrawn), Amazon, Microsoft	50 million	Drones	Acquisition of AI technologies for reconnaissance of images from military drones
2020 – CIA	Alphabet, Amazon, Microsoft, Oracle	Multi-billion	Cloud	Cloud services for 17 intelligence agencies
2021 – DoD; HoloLens	Microsoft (withdrawn)	21,9 billion	Visors and augmented reality	HoloLens augmented reality headsets for military activities in highly complex environments
2022 – NSA; Wild and Stormy project	Amazon	10 million	Cloud	NSA Cloud infrastructure
2022 – DoD	Microsoft	n.a.	Stryker armoured vehicles	Digital systems to be included in Army armoured vehicles
2022 – DoD	Alphabet (Google public sector division)	n.a.	Google workspace	Provision of Google Workspace systems to 250,000 DoD employees
2022 – DoD; Joint Warfighting Cloud Capability	Alphabet, Amazon, Microsoft, Oracle	9 million	Cloud	Defence Cloud infrastructure
2022 – DoD; Hybrid Space Architecture programme	Amazon, Microsoft	n.a.	Satellites	Space and land infrastructure for national security
2023 — SSC/ DoD	Microsoft	19.8 million	Cloud-based space simulation (viewable with Microsoft HoloLens headsets)	Space simulator aimed at gaining situational awareness and acting faster than adversaries
2024 — DoD	Amazon	22 million	Cloud	Cloud services for the Army department of the US Special Operations Command
2024 – DoD / Air Force	Amazon	29,3 million	Cloud / cyber systems	Cloud services for Air Force defensive cyber systems
2024 – DoD / Air Force	Amazon	25,6 million	Cloud	Global Warfighting Cloud Infrastructure
2025 – DoD / DISA	Amazon	17,7 million	Cloud	F-35 Lightning II Joint Program Office.
2026 – Department of Homeland Security	Amazon	2,5 billion	Cloud	Cloud contract covering IaaS, PaaS, SaaS, professional services and training support

Source: Adaptation from Coveri et al. (2025b); Notes: DoD refers to Department of Defence; DISA stands for Defence Information Systems Agency; DCSA for Defence Counterintelligence and Security Agency.

The close relationship between Big Tech and the military and intelligence apparatuses is confirmed by the extent of the revolving doors through which former Big Tech executives occupy top appointments in defence-and intelligence-related agencies while former military officers or federal officials move in the opposite direction. Coveri et al. (2025a) have documented in detail the revolving-door dynamics (e.g., Doug Beck, former vice-president of Apple, in 2023 appointed as the new director of the Pentagon's Defense Innovation Unit or Eric Schmidt, former CEO of Alphabet who served as chairman of the Defense Innovation Advisory), emphasising how such movements allow the transfer of high-level competences, of tacit knowledge and – more generally – of values and modes of behaviour between business and government, contributing to a convergence in the interests and strategies of both sets of actors (Lundvall and Rikap, 2022). By the same token, government officials and policymakers are an important asset for Big Tech insofar as they can provide insider knowledge of how government agencies function, how legislation and regulation evolve, and which programmes and contracts are being launched in military sectors.

Another distinctive feature of the military–digital complex is the direct involvement of major technology companies in battlefield operations. There have been numerous documented cases. For example, SpaceX, Amazon and Microsoft played a crucial role in Ukraine by providing the military with connectivity, managing government data on their servers, and supplying cyber-attack defence systems. Amazon, Google and Microsoft's cloud and AI systems were also used by the Israeli Defence Forces to conduct operations in Gaza, while the AI systems of Anthropic and Palantir played a decisive role in US military actions in Venezuela and Iran. Conversely, a few days after the US and Israeli attack, the Iranian military bombed Amazon and Microsoft data centres in Bahrain and the United Arab Emirates.

As a sort of new East India Company, Big tech firms are effectively becoming 'digital mercenaries' that can benefit significantly from participating directly in military activities. First, they strengthen their bargaining power with the government. The more essential—and difficult to replicate or substitute—their tools are (e.g., Palantir's defence platform), the easier it becomes to secure new military contracts and the harder it is for hostile policies or regulations to challenge their position. Second, the battlefield is an extremely valuable environment for testing and refining new applications, paving the way for learning and the accumulation of capabilities that can be utilised in both military and civilian contexts.

In the US, this represents a critical reshaping of the traditional military-industrial complex. The role of legacy defence contractors is being scaled back, as an increasing share of the Pentagon's budget is being channelled to Big Tech companies, on which—as noted—they also depend for the digital components of their equipment and weaponry. Unlike traditional defence contractors who build physical hardware (e.g., fighter jets) that is subsequently owned, operated, and commanded by sovereign military personnel, Big Tech retains ownership and operational control over the digital infrastructure (cloud computing, satellite constellations, AI algorithms). This may create a severe 'hold-up problem'. Once a government migrates its classified military data and operational capabilities onto a proprietary commercial cloud, it becomes structurally locked in. The state is then vulnerable to extortionate rent-seeking, as the digital mercenary can unilaterally change the terms of service, raise prices, or restrict access to critical infrastructure. As a result, the intelligence and military apparatuses become structurally dependent on the proprietary cybersecurity protocols, software updates, and server maintenance schedules dictated by private corporations. The government's dependence may become so intense that Big Tech companies can use their involvement in conflicts as a strategic lever (Hammond-Errey, 2026). A notable precedent is SpaceX's decision to geofence its Starlink satellite network in Ukraine in 2022, effectively demonstrating that a private CEO possesses the unilateral capability to alter a sovereign state's military operations.

The prominent role of Big Tech in the military-digital complex lends support to Abels (2026)'s hypothesis of a 'privatised technological sovereignty'. This is a structural challenge that transcends borders and affects almost all states. Even technological superpowers like the US increasingly find their sovereign capabilities mediated by private actors, relying heavily on commercial mega-platforms to provision critical defence cloud architectures (e.g., AWS or Microsoft) or to secure vital orbital access and communications (e.g., SpaceX). Structural (e.g., strength of the national system innovation system) and institutional heterogeneities matter, though. While the US delegates state functions solely to domestic monopolies, the Chinese government has coercive and planning tools at its disposal that can more easily enable it to align national Big Tech with its strategic objectives, this vulnerability becomes particularly acute in regions like the EU.

Lacking native tech giants capable of rivaling their US or Chinese counterparts, the EU is, as documented, fundamentally dependent on foreign actors to access critical infrastructures and technologies. On the other hand, attempts to artificially engineer strategic autonomy through public-private partnerships and concession models may make the pursuit of technological sovereignty equally difficult. Analysing the recent Iris2 project[7], Abels (2026) shows that by relying on 'financial de-risking', heavily subsidizing corporate R&D and guaranteeing long-term procurement contracts to incentivize private investment in strategic infrastructures (e.g., sovereign cloud initiatives or secure satellite constellations like Iris2), the EU absorb massive financial risks while ceding technological control and intellectual property to an increasingly concentrated private sector. Driven by the aim of reducing dependence on foreign players, such a massive reliance on private capital may fundamentally compromise the objective of sovereignty. De-risking strategies may end up socialising the immense financial risks of developing critical technologies, while the technological capabilities, intellectual property, and ultimate control remain privatised.

The perverse intertwining of power within the US military-digital complex, as well as the subordination of European space procurement to private capital documented by Abels (2026), makes one thing abundantly

[7] The IRIS2 project entails a new multi-orbital constellation of Medium Earth and Low Earth Orbit 290 satellites set to provide secure connectivity services to the EU and its Member States as well as broadband connectivity for governmental authorities and private companies.

clear: *technological sovereignty cannot be purchased off-the-shelf*. By outsourcing the critical defence infrastructures to Big Tech, states are not merely engaging in a novel form of public procurement; they are effectively reverting to a modernized, digital system of mercenary defence. Likewise, when the state as in the EU case attempts to secure technological autonomy by relying on de-risking mechanisms and local private monopolies, it does not develop sovereign capabilities but rather risks to permanently privatise the power to dictate the future trajectory of strategic technologies.

In the next section, we propose a typology that illustrates how the systemic power of digital corporations and their growing centrality to military activities can influence the pursuit of TS in different ways, depending on infrastructural and technological capabilities and on the nature of state–corporate relations.

4. Technological sovereignty at the time of the military-digital complex: a typology

In the context depicted in the previous sections, we argue that the very concept of TS requires substantial refinement, loosening an assumption that still shapes much of the literature (Edler et al., 2023): the idea that the sovereign subject is, almost by definition, the state. As control over critical infrastructures and technologies is often exercised by private corporations, public-private consortia or hybrid state-platform arrangements, the relevant question is therefore not only whether a country has TS, but who exercises it, through which governance mechanisms, and with what consequences for welfare, democratic accountability and long-term structural capabilities (Rolf and Schindler, 2023).

A first fundamental structural divide must be highlighted: on the one hand, economies that possess critical digital infrastructure (or, at least, that are not subordinate actors across most parts of the digital stack) and technologies (along with the idiosyncratic capabilities accumulated during their development), on which a significant share of private and public activities—including military ones—now depend; on the other hand, those that depend, to varying degrees, on foreign entities such as Big Tech (Abels, 2026). In fact, while complete digital self-sufficiency is unattainable due to the global distribution of raw materials, components, and technologies, a clear distinction can nevertheless be drawn between those economies capable of ‘weaponising’ interdependencies (Farrel and Newman, 2019) on the basis of their assets and capabilities (as well as leveraging the ‘special relationship’ with key corporations such as Big Tech), and those subordinate to the technological capabilities of others and therefore more susceptible to coercive action.

The second fault line concerns the nature of the relationship between the state and private capital, which produces significant heterogeneity in governance structures. Although the presence of private entities of systemic importance that control critical infrastructure and technologies is a defining feature of contemporary capitalism (Rikap, 2024), the nature of their relationship with the state—and the state’s ability to regulate their activities—varies across countries and reflects the characteristics of national innovation and governance systems (Kontareva and Kenney, 2024; Schindler and Rolf, 2025). The same elements—for example, the presence or absence of state-owned enterprises in key sectors, the scope and selectivity of industrial policy, and the stringency of regulations governing the use of new technologies for ethically and socially sensitive purposes (such as restrictions on access to personal or sensitive data and digital surveillance)—can shape the capacity of economies that interact with, and experience varying degrees of dependence on, Big Tech to manage this relationship and, above all, to mitigate the negative consequences of technological and infrastructural dependence (Calvo et al., 2025).

Table 6. A typology of technological sovereignty: governance drivers

	Private-driven	Public-driven	Public-private driven
Strong Technological Sovereignty	**Market-led sovereignty** • Private Big-Tech companies' dominance • Low regulation/light-touch oversight • Strong proprietary platforms • Large-scale private R&D and data control • Fast innovation, but dependency and lock-in risks • Strategic autonomy mediated by corporate interests; privatization of security and military domains	**State-led sovereignty** • State-owned or publicly controlled enterprises • Public development financial institutions • Mission-oriented industrial policy • Strategic public procurement • Public control of critical infrastructure • National champions and vertical policy • Security-driven technology priorities	**Co-governed sovereignty** • State-owned enterprises + Big Tech capabilities • High regulation and public conditionality • Joint ownership of critical patents/data • Public-private investment platforms • Regulated cloud, AI and digital infrastructure • Strategic coordination across security and industry
Weak Technological Sovereignty	**Corporate dependency** • Foreign private platforms controlling key infrastructures/services • Government's weak bargaining position • Vendor lock-in and proprietary standards • Data extraction and value transfer abroad • Limited domestic technological capabilities • Privatization of security and military domains with foreign dependency	**State fragility** • Formal public control, weak capabilities • Underfunded public R&D and procurement • Fragmented institutions/poor coordination • Technology nationalism without scale • Inefficient state firms or legacy infrastructures	**Dependent hybrid regime** • Public-private partnerships without autonomy • Regulation exists but enforcement is weak • Public sector reliant on foreign Big Tech • Procurement reinforces external dependencies • Fragmented standards and limited interoperability • Shared governance, asymmetric power

Source: Authors' elaboration.

Building on these to demarking lines we propose a typology of TS which is summarized in Table 6. The vertical axis distinguishes strong and weak TS. Strong TS refers to the presence of domestic or allied capabilities, strategic bargaining power and a meaningful degree of control over critical infrastructures and technological trajectories. Weak TS points instead to dependency, limited bargaining power, fragmented capabilities, or a gap between formal authority and effective control. The horizontal axis identifies the prevailing governance framework: private-driven, public-driven and public-private driven. This dimension matters because similar levels of technological capability may generate very different political-economic outcomes depending on whether strategic assets are controlled by public institutions, domestic Big Tech, foreign platforms, state-owned enterprises or public-private consortia. The proposed typology is not intended to identify a set of ideal types, neither as a rigid country classification scheme, though, as it will be highlighted, some specific country features can be interpreted according to this conceptual framework. Its purpose is to develop an analytical scheme that aims to elaborate on the concept of TS in order to account for the structural characteristics and transformations of different economic systems.

Strong private-driven TS: market-led sovereignty

The upper-left cell describes a configuration in which technological capabilities are very strong, while sovereignty is largely mediated by private corporations. The United States is the clearest example. Its position in cloud computing, AI, software, semiconductor design, digital platforms and satellite communications is exceptionally strong. Yet many of the infrastructures that enable public and military power are owned and operated by firms such as Microsoft, Amazon, Google, Meta, Palantir and SpaceX. In this setting, the state preserves geopolitical and regulatory power, but the operational means of sovereignty are increasingly supplied by private actors. This arrangement can sustain rapid innovation and technological scaling, since firms mobilise large R&D budgets, proprietary datasets, specialised labour and global platform

ecosystems. At the same time, public authority becomes dependent on corporate architectures and on private incentives that do not necessarily overlap with collective objectives.

The welfare balance is therefore ambiguous. Market-led sovereignty may accelerate innovation, diffusion and productivity in frontier domains. It may also orient technological change towards commercially appropriable applications, military contracts and data-intensive services, rather than towards public health, green transition, educational infrastructures or other public-goods-related domains. A further risk is the privatisation of structural capabilities. Public authorities purchase access to cloud, AI or satellite systems without rebuilding the internal capacity to design, own and govern them. In essential sectors, this may turn the state into a tenant of privately-owned infrastructures. The resulting lock-in can increase fiscal costs, reduce policy autonomy and reinforce rent extraction by intellectual monopolies (Coveri et al., 2022, 2025a). In dual-use technologies, the problem becomes even sharper: private firms may acquire de facto leverage over security-related choices, as discussed in the previous sections. In this configuration, the convergence between the military apparatus and Big Tech—driven both by the digitalisation of warfare and by the growing importance of military spending for the profits of major platforms—fosters the privatisation of war and may consolidate the power of Big Tech (albeit within an unstable and conflict-ridden context, both in terms of state–Big Tech relations and competition among the latter, Rikap, 2025), while also steering technological development towards surveillance and the refinement of instruments of war (Guarascio and Pianta, 2025).

Strong public-driven TS: state-led sovereignty

The upper-middle cell refers to a configuration in which the state directly controls the main instruments of technological development. This may take place through state-owned enterprises, public research organisations, public development banks, mission-oriented industrial policy, strategic procurement and direct control of critical infrastructures. This is the closest to the classical understanding of sovereignty: public authority defines strategic priorities, allocates resources and retains control over assets that are essential for collective security and welfare. Historical examples include large public R&D programmes, military and space agencies, public laboratories and infrastructure enterprises. In Europe, experiences such as Airbus, Ariane, CERN-related research infrastructures and some national public digital infrastructures show that state-led or publicly coordinated technological capabilities can be built when scale, finance and institutional coordination are adequate.

China also presents elements of state-led sovereignty, especially where the party-state directs investment, regulates data flows, controls platforms and aligns firms with national strategic priorities (Rolf and Schindler, 2023). The main advantage of public-driven TS is its potential to connect technological trajectories with collective priorities such as resilience, industrial upgrading, territorial cohesion and universal access to essential services. Its main limits are organisational and institutional. Public control without adequate capabilities can become formal sovereignty without substantive autonomy. Bureaucratic inertia, underfunded R&D, weak procurement capacity and fragmented public agencies may prevent ownership from becoming innovation. Welfare gains therefore depend on the combination of public authority, technical competence, long-term finance, openness to scientific collaboration and institutional accountability.

Strong public-private-driven TS: co-governed sovereignty

The upper-right cell concerns arrangements in which technological sovereignty is produced through structured coordination between public authorities and private actors. China is again the most relevant contemporary case of a strong hybrid configuration (Jia and Kenney, 2022). Its major digital firms are commercially dynamic, but they operate within a dense framework of party-state steering, industrial policy, data regulation and security priorities. This model differs from US market-led sovereignty because private platforms are more directly subordinated to strategic state objectives (although the relationship is complex and characterised by alternating phases of conflict and cooperation, see To, 2023). It also differs from pure public sovereignty because technological development still depends heavily on corporate capabilities,

competition among national champions and private accumulation strategies. The Chinese case therefore points to a form of TS generated by a state-platform nexus, rather than by the state or the market alone.

The EU also seeks forms of co-governed sovereignty, although from a weaker position. Programmes in semiconductors, cloud, secure satellite communications and digital infrastructures combine public funding, regulation and industrial coordination, but they often rely on private consortia and incumbent firms (Abels, 2026). The crucial issue is whether public-private governance is accompanied by strong public conditionality: joint ownership of critical patents and data, interoperability obligations, public audit rights, open standards, domestic capability-building and credible exit options from proprietary systems (Di Carlo et al., 2026). Without these conditions, public-private cooperation risks becoming financial de-risking rather than sovereignty-building. The welfare concern is that the public sector socialises costs while strategic control, intellectual property and future rents remain private. Co-governed sovereignty can therefore be welfare-enhancing only when public institutions are able to discipline private actors and embed their capabilities within public missions.

Weak private-driven TS: corporate dependency

The lower-left cell is particularly relevant for the European debate. It describes a situation in which key infrastructures and services are controlled by foreign private platforms, while the domestic state has limited bargaining power. Many EU member states approximate this condition in cloud computing, AI services, data infrastructure and some defence-related digital services. The EU has strong regulatory authority through instruments such as the GDPR, the Digital Markets Act and the Digital Services Act. However, regulatory power does not automatically translate into technological capability. When public administrations, firms, universities, hospitals or defence agencies depend on foreign hyperscalers for data storage, compute capacity and software ecosystems, TS remains fragile despite formal legal autonomy.

The welfare drawbacks are substantial. Corporate dependency can transfer value added, data and strategic knowledge abroad; increase exposure to extraterritorial legislation; reduce domestic learning; and constrain the emergence of local suppliers. It can also erode structural capabilities in essential sectors. If health data infrastructures, public administration platforms, educational cloud services or defence communication systems are outsourced to foreign proprietary providers, public institutions may lose the skills, routines and organisational memory required to govern those systems (Cirillo et al., 2025). This is a developmental issue as much as a security issue. Technological trajectories become shaped by the product roadmaps and profitability requirements of external firms, while the domestic economy is pushed towards adoption rather than production. Under these conditions, private-driven TS may obstruct welfare-enhancing innovation by reinforcing dependency and weakening the public capacity to define collective priorities.

Weak public-driven TS: state fragility

The lower-middle cell refers to cases in which the state formally claims control over technological development but lacks the resources, coordination capacity or industrial base needed to make that control effective. This can occur when countries adopt technology nationalism without scale, invest in isolated public projects without a coherent industrial ecosystem, or rely on legacy state firms unable to operate at the frontier. Russia illustrates some aspects of this configuration outside its traditional strengths in military, nuclear and space technologies (Kontareva and Kenney, 2024). Strategic isolation and sanctions may strengthen state rhetoric and import-substitution efforts, but they can also restrict access to advanced components, frontier research networks and global markets, reducing both the quality and diffusion of innovation. Some EU initiatives may also move in this direction when fragmentation across member states, limited fiscal capacity and weak coordination prevent public programmes from reaching scale.

From a welfare perspective, state fragility entails significant opportunity costs. Public resources are mobilised in the name of sovereignty, but without scale or absorptive capacity they may support inefficient incumbents, duplicate infrastructures or symbolic projects with limited spillovers. This can crowd out investment in education, basic research, public digital capabilities and industrial upgrading. It can also produce technological nationalism without social returns: the state controls assets that are neither innovative nor broadly useful. The policy implication is straightforward. Public-driven TS requires more than ownership

or public procurement. It requires cumulative capability-building, technical skills inside public administrations, coordination across research and industry, and a macroeconomic framework capable of sustaining long-term investment.

Weak public-private-driven TS: dependent hybrid regime

The lower-right cell identifies situations in which public-private partnerships exist, but the balance of power remains asymmetric and dependency is not resolved. This is a concrete risk for the EU if its strategy relies on concessions, subsidies and industrial alliances without strong public ownership, open standards and credible technological alternatives. Public-private partnerships can be useful when they bring together complementary capabilities (Mazzucato and Rodrik, 2026). They become dependent hybrid regimes when public authorities provide demand, guarantees and subsidies while private actors retain the strategic assets. In such cases, procurement may end up reinforcing the dependencies it was meant to reduce. A sovereign cloud initiative tied to foreign hyperscalers, or a secure satellite system in which public authorities bear the financial risk while private actors appropriate ownership and commercial rents, would fall into this category.

The welfare implications are serious because dependent hybridity combines weaknesses of both state and market. The public sector absorbs risks and fiscal costs, while private firms retain control over technological choices, intellectual property and future revenue streams. Citizens may pay twice: first through public subsidies and then through fees, procurement contracts or monopoly rents. In addition, the developmental trajectory may shift towards commercially profitable technologies rather than infrastructures with high social returns. Essential sectors - health, education, mobility, energy, public administration and defence - are especially exposed because they require long-term, interoperable and accountable systems. When these systems are governed through asymmetric public-private arrangements, structural capabilities may be progressively privatised and hollowed out within the public sector.

5. Conclusions

This paper has examined TS at a historical moment in which the control of critical technologies, infrastructures and knowledge is increasingly concentrated in a limited number of digital corporations. Its starting point was a conceptual tension in the existing debate. TS is commonly defined as the capacity of a state, or a federation of states, to access and provide critical technologies without incurring one-sided structural dependence (Edler et al., 2023). Yet this definition implicitly assumes that sovereignty is ultimately held and exercised by public authorities. The argument developed in the present paper is that this assumption has become increasingly problematic. In core domains such as cloud computing, AI, data infrastructures, satellite systems and digital services for defence, the effective control of technological capabilities is often exercised by private corporations whose interests, strategies and governance mechanisms only partly overlap with public objectives.

The empirical evidence discussed in the paper points to three connected transformations. First, the long-term retreat of public research and the expansion of intellectual property regimes have shifted the centre of gravity of innovation systems towards large private actors. The rise of ICT and platform-based business models has reinforced this tendency by allowing a small group of firms to accumulate data, proprietary knowledge, network advantages and infrastructural assets on a global scale. Second, the hierarchy of corporate R&D has changed substantially since the early 2000s. Digital firms, especially from the United States and China, now occupy the leading positions among global R&D spenders and dominate strategic technological areas such as AI, cloud and software ecosystems. Third, this concentration is infrastructural as much as technological. The control of data centres, cloud availability zones, platforms, operating systems and search engines gives Big Tech firms a systemic role in the functioning of economies, public administrations and security apparatuses (Coveri et al., 2025).

As a result, this concentration of techno-economic power modifies the relationship between the state and private capital. Public authorities no longer simply procure technologies from firms operating in competitive markets. In many cases, they depend on proprietary ecosystems that set standards, store data, provide

computing capacity, update software and mediate access to essential digital functions. This produces a form of structural lock-in that is particularly severe in dual-use and security domains. The state can retain formal authority while losing part of the operational capacity required to exercise it. Under these conditions, TS cannot be evaluated only by measuring the presence of advanced technologies within a territory; it must also be assessed by asking who owns, controls and governs the infrastructures and knowledge through which those technologies are produced and deployed.

The analysis of the military-digital complex further strengthens this conclusion (Guarascio and Pianta, 2025). The digitalisation of warfare has made the capabilities of Big Tech increasingly indispensable for military and intelligence activities. Cloud infrastructures, AI systems, cyber-defence tools, satellite connectivity and battlefield data services have become essential components of contemporary security systems. At the same time, public procurement, defence contracts and battlefield experimentation reinforce the technological and market position of these firms. Hence, the resulting relationship is one of mutual dependence, but it is not necessarily symmetrical. Governments need access to digital infrastructures and capabilities that they often do not control internally, while Big Tech firms use military and security demand to consolidate their technological advantages, expand proprietary ecosystems and increase their bargaining power vis-a-vis public authorities. This gives concrete substance to the notion of privatised TS (Abels, 2026).

Building on this analytical and empirical framework, the paper proposes a typology for interpreting the notion of TS according to these structural transformations. In particular, it distinguishes between strong and weak technological sovereignty and between private-driven, public-driven and public-private-driven governance arrangements. This distinction matters because the same technological capability may have different economic and political implications depending on the distribution of control across states, domestic firms, foreign firms and hybrid institutional arrangements.

Taken together, these findings suggest that TS should not be assessed only by asking whether a country possesses advanced technologies. It should also be assessed by examining how control is distributed and governed across the state, domestic firms, foreign firms and hybrid governance arrangements. The broader implication is that private-driven TS is not neutral from a welfare standpoint. It may increase innovation speed and geopolitical capacity, but it can also redirect technological change towards rent extraction, militarisation and proprietary lock-in. On the opposite, public-driven technological sovereignty can better preserve public-good objectives, but public institutions should possess adequate technical, financial and organisational capabilities, while public-private technological sovereignty can work when public conditionality is strong; otherwise, it may degenerate into the socialisation of risk and the privatisation of control. A welfare-oriented strategy for TS should therefore prioritise public and collective control over essential technological infrastructures, strengthen public R&D and procurement capabilities, impose interoperability and open-standard requirements, and ensure that critical data, patents and infrastructures generated with public support remain accessible for public purposes.

The central policy question, therefore, is not simply how to become technologically sovereign, but how to prevent the pursuit of sovereignty from becoming a vehicle for the privatisation of the very capabilities on which welfare, democracy and long-term development depend. Technological sovereignty can strengthen resilience, strategic autonomy and collective welfare only if it is embedded in institutions capable of governing technological change in the public interest. Without such institutions, the language of sovereignty may legitimise new forms of dependency: dependence on domestic monopolies in some countries, dependence on foreign platforms in others, or dependence on public-private arrangements in which public authorities finance strategic projects while private actors retain control over their future trajectories. A research and policy agenda on TS should therefore place ownership, governance and accountability at the centre of the analysis, alongside capabilities and geopolitical positioning.

References

Abels, J. (2026). Privatised technological sovereignty: the IRIS² space project and state-capital relations in the European Union. *Journal of European Public Policy, 1-28.*

Andreoni, A. and Chang, H. J. (2019). The political economy of industrial policy: Structural interdependencies, policy alignment and conflict management. *Structural change and economic dynamics, 48, 136-150.*

Archibugi, D. and Mariella, V. (2021). Is a European recovery possible without high-tech public corporations?. *Intereconomics, 56(3), 160-166.*

Archibugi, D., & Filippetti, A. (2018). The retreat of public research and its adverse consequences on innovation. *Technological Forecasting and Social Change*, *127*, 97-111.

Arenas Díaz, G., Piva, M., & Vivarelli, M. (2025). *Artificial intelligence as a method of invention* (No. 1676). GLO Discussion Paper.

Beraja, M., Peng, W., Yang, D. Y., & Yuchtman, N. (2025). Government as venture capitalists in artificial intelligence. Entrepreneurship and innovation policy and the economy, 4(1), 81-102.

Bianchini, S., Müller, M., & Pelletier, P. (2022). Artificial intelligence in science: An emerging general method of invention. *Research Policy*, *51*(10), 104604.

Calvano, E., & Polo, M. (2021). Market power, competition and innovation in digital markets: A survey. *Information Economics and Policy*, 54, 100853.

Calvo, A. G., Kenney, M., & Zysman, J. (2025). Responding to platform firm power: differing national responses. New political economy, 30(2), 225-239.

Caravella, S., Crespi, F., Cucignatto, G. and Guarascio, D. (2024). Technological sovereignty and strategic dependencies: The case of the photovoltaic supply chain. *Journal of Cleaner Production, 434, 140222.*

Cirillo, V., Durand, C., Guarascio, D., Rabinovich, J. and Rikap, C. (2025). Power, knowledge and technology in a finite world. *Review of Political Economy, 37(4), 1467-1478.*

Conyon, M., Ellman, M., Pitelis, C. N., Shipman, A., & Tomlinson, P. R. (2022). Big tech oligopolies, Keith Cowling, and monopoly capitalism. *Cambridge Journal of Economics*, *46*(6), 1205-1224.

Coveri, A., Cozza, C. and Guarascio, D. (2022). Monopoly Capital in the time of digital platforms: a radical approach to the Amazon case. *Cambridge Journal of Economics, 46(6), 1341-1367.*

Coveri, A., Cozza, C. and Guarascio, D. (2025a). Blurring boundaries: an analysis of the digital platforms-military nexus. *Review of Political Economy, 37(4), 1632-1663.*

Coveri, A., Cozza, C. and Guarascio, D. (2025b). Big Tech and the US Digital-Military-Industrial Complex. *Intereconomics, 60(2), 81-87.*

Crespi, F. and Guarascio, D. (2019). The demand-pull effect of public procurement on innovation and industrial renewal. *Industrial and Corporate Change, 28(4), 793-815.*

Crespi, F., Caravella, S., Menghini, M. and Salvatori, C. (2021). European technological sovereignty: an emerging framework for policy strategy. *Intereconomics, 56(6), 348-354.*

Crespi, F., Cerra, R. and Zezza, F. (2025). Coopetitive Technological Sovereignty: A Strategy to Reconcile International Collaboration with Knowledge and Economic Security. *Intereconomics, 60(2), 73-80*.

Culpepper, P. D., & Thelen, K. (2020). Are we all Amazon primed? Consumers and the politics of platform power. *Comparative Political Studies*, 53(2), 288-318.

Di Carlo, D., McNamara, K. and Moschella, M. (2026) The New Politics of EU Industrial Policy: From the Regulatory State to a Transformational State, *Governance.*

Edler, J. and Fagerberg, J., (2017). Innovation policy: what, why, and how. *Oxf. Rev. Econ. Policy 33 (1), 2–23.*

Edler, J., Blind, K., Frietsch, R., Kimpeler, S., Kroll, H. and Lerch, C. (2020). Technology Sovereignty: from demand to concept. *Perspectives-Policy Brief. Karlsruhe 27.*

Edler, J., Blind, K., Kroll, H. and Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means. *Research Policy, 52(6), 104765.*

Fanti, L., Guarascio, D., & Moggi, M. (2022). From Heron of Alexandria to Amazon's Alexa: a stylized history of AI and its impact on business models, organization and work. *Journal of Industrial and Business Economics*, *49*(3), 409-440.

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. International security, 44(1), 42-79.

Farrell, H. and Newman, A. (2023) *Underground empire: How America weaponized the world economy*. Random House.

Durand, C., & Milberg, W. (2020). Intellectual monopoly in global value chains. *Review of International Political Economy*, 27(2), 404-429.

Gawer, A., & Cusumano, M. A. (2014). Industry platforms and ecosystem innovation. *Journal of product innovation management*, 31(3), 417-433.

Gineikyte-Kanclere, V. et Al., *2025, European Software and Cyber Dependencies*, publication for the Committee on Industry, Research and Energy, Policy Department for Transformation, Innovation and Health, European Parliament, Luxembourg.

Gjesvik, L. (2023). Private Infrastructure in Weaponized Interdependence. *Review of International Political Economy, 30(2): 722–746.*

Gjesvik, L. (2023). Private infrastructure in weaponized interdependence. *Review of International Political Economy*, 30(2), 722-746.

González, R. J. (2023). Militarising Big Tech. The rise of Silicon Valley's digital defence industry. *Transnational Institute. Available at: https://www.tni.org/files/2023-04/Militarising%20%20Big%20Tech.pdf*

Greenstein, S. (2000). Commercialization of the Internet: The interaction of public policy and private choices or why introducing the market worked so well. *Innovation policy and the economy*, *1*, 151-186.

Guarascio, D. (2026) *Imperialismo Digitale. Economia e Guerra ai Tempi delle Piattaforme e dell'IA*, Bari/Roma: Laterza.

Guarascio, D. and Pianta, M. (2025). Digital technologies: civilian vs. military trajectories (No. 2025/08). *LEM Working paper series.*

Harper, J. (2020). Defense innovation unit shifts into higher gear. *National Defense, 104(795), 20-21.*

Jacobides, M. G., Cennamo, C., & Gawer, A. (2024). Externalities and complementarities in platforms and ecosystems: From structural solutions to endogenous failures. *Research Policy*, *53*(1), 104906.

Jia, K., & Kenney, M. (2022). The Chinese platform business group: an alternative to the Silicon Valley model?. Journal of Chinese governance, 7(1), 58-80.

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

Kenney, M., and J. Zysman (2020) The Platform Economy: Restructuring the Space of Capitalist Accumulation. *Cambridge Journal of Regions, Economy and Society 13 (1): 55–76.*

Kontareva, A., & Kenney, M. (2024). Building national autonomy in a platform-dominated world: Russia state policy towards platforms.

Larouche, P. and De Streel, A. (2021). The European digital markets act: A revolution grounded on traditions. *Journal of European Competition Law & Practice, 12(7), 542-560.*

Letta, E. (2024) Much more than a market https://www.con-silium.europa.eu/media/ny3j24sm/much-more-than-a-mar-ket-report-by-enrico-letta.pdf (last accessed 3.5.2024)

Mazzucato, M. and Rodrik, D. (2026). Industrial policy with conditionalities: a taxonomy and sample cases. *Industrial and Corporate Change*, dtaf063.

Mowery, D. (2010) *Chapter 29 - Military R&D and Innovation*, in Hall, B. and Rosenberg N. (eds) *Handbook of the Economics of Innovation*, Volume 2, pp.1219-1256, Amsterdam: North Holland.

Mowery, D. C. (2009). Plus ca change: Industrial R&D in the "third industrial revolution". Industrial and corporate change, 18(1), 1-50.

Mowery, D. C., & Nelson, R. R. (Eds.). (1999). *Sources of industrial leadership: studies of seven industries*. Cambridge University Press.

O'Mara, M. (2020). *The code: Silicon Valley and the remaking of America*. Penguin.

Pagano, U. (2014). The crisis of intellectual monopoly capitalism. *Cambridge Journal of Economics*, *38*(6), 1409-1429.

Pagano, U. (2026). The corporation from the Middle Ages to intellectual monopoly capitalism. Journal of Institutional Economics, 22, e16.

Pagano, U., & Rossi, M. A. (2009). The crash of the knowledge economy. Cambridge Journal of Economics, 33(4), 665-683.

Rahman, K. S. and Thelen, K. 2019. The rise of the platform business model and the transformation of twenty-first-century capitalism, Politics & Society, vol. 47, no. 2, 177–204

Rikap, C. (2024). Intellectual monopolies as a new pattern of innovation and technological regime. *Industrial and Corporate Change*, *33*(5), 1037-1062.

Rikap, C., & Lundvall, B. Å. (2021). *Digital innovation race*. London: Springer International Publishing.

Rolf, S. and Schindler, S. (2023). The US–China rivalry and the emergence of state platform capitalism. *Environment and Planning A: Economy and Space, 55(5), 1255-1280.*

Schindler, S., & Rolf, S. (2025). Geostrategic globalization: US–China rivalry, corporate strategy, and the new global economy. Globalizations, 22(6), 897-914.

Sun, J., & Kenney, M. (2025). Beyond Catch-up: State-led Decentralized National Innovation System and the Rise of Emerging Industries in China. *Available at SSRN 6651378*.

To, Y. (2023). Friends and foes: Rethinking the party and Chinese big tech. New Political Economy, 28(2), 299-314.

Uyarra, E. and Flanagan, K. (2010). Understanding the innovation impacts of public procurement. *European planning studies, 18(1), 123-143.*

Zuboff, S. (2019). *The age of surveillance capitalism*. Profile Books.