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

Digital technologies: civilian vs. military trajectories

Dario Guarascio [a]
Mario Pianta [b]

[a] Sapienza University of Rome, Italy
[b] Scuola Normale Superiore, Florence, Italy

2025/08 March 2025
ISSN(ONLINE): 2284-0400
DOI: 10.57838/sssa/dkb0-wb35

Digital technologies:
civilian vs. military trajectories

Dario Guarascio[*], Sapienza University of Rome,
Mario Pianta, Scuola Normale Superiore, Florence

Abstract

The article examines the evolution of the current technological paradigm, based on digital technologies, considering the interaction between civilian and military trajectories, with a focus on the US case. Building on an original political economy framework, the activities of corporations and the industrial and technology policies of the US government are examined.

The evolution of digital technologies and the rise of major US corporations - Alphabet, Amazon, Apple, Meta, Microsoft – is investigated, showing that their platform business model is characterised by monopoly power, management of Big Data and major capabilities of control, surveillance and targeting. A civilian trajectory – with large commercial markets and a novel reach in several areas of social activities - has dominated the rise of digital technologies. Its key characteristics, however, have become of major interest for military priorities.

The analysis of recent US industrial and technology policies for the military shows that they have expanded the involvement of US digital corporations in arms and security programmes, developed large defense R&D projects in digital areas, and shaped a new convergence between civilian and military trajectories. The outcome we are facing is therefore the emergence of a *digital-military-industrial complex* - a major and problematic novelty in a digital age that had grown out of a civilian trajectory.

Keywords: digital technologies, technological trajectories, military programs.
JEL codes: O30, O33, 038

1. Technological paradigms, civilian and military trajectories

In this article we investigate how, in our digital age, corporate strategies and government industrial and technology policies shape its orientation towards civilian or military goals. Such questions are at the crossroads between scolarhips focusing on technology (Schumpeter 1961, Rosenberg 1982, Dosi et al. 1988, Dosi, 2023), military-civilian relationships (Kaldor, 1982, Tirman, 1984, Smith, 1985, Mowery, 2010), and political economy perspectives on technology (Strange, 1984, Noble, 1984, Pianta, 1988, Zuboff, 2019).

The starting point is the concept of *technological paradigms* (Perez, 1983, Freeman and Perez, 1988, Freeman and Louçã, 2001). The sequence of long cycles of economic growth since the industrial revolution have been associated to a specific set of technologies, characterised by rapidly declining

[*] Corresponding author: dario.guarascio@uniroma1.it

prices and growing performances, and by a high pervasiveness in the economy and society. The early 20th century has been dominated by the ‘Fordist’ mechanical and chemical technologies of mass production, shaping industrialisation and mass consumption. Since the 1980, a new paradigm based on Information and Communication Technologies (ICTs) has emerged, that has now evolved in our current digital age.

Building on the definition of 'scientific paradigm' by Thomas Kuhn (1962), Giovanni Dosi argued that a 'technological paradigm' can be seen as “a ‘model’, and a ‘pattern’ of solution of technological problems, based upon principles derived from natural sciences and on selected material technologies” (Dosi 1982: 152). In the case of semiconductors, in order to perform a generic task (amplifying and switching electrical signals) a material technology is selected (silicon semiconductors), which uses specific scientific properties, and allows a progressive improvement of performances.

The diffusion of technological paradigms in the economy and society is summarised by Carlota Perez (1983: 366). First, 'radical breakthroughs' in a new technology make new forms of production possible. Second, the economic structure is transformed, with the growth of new sectors, different inter-industry relations and the development of new products, processes and forms of organization. Third, the labour force is reorganized, with changes in the labour process, in the composition and skills of the workforce. Fourth, the social structure is reshaped, with a new wage and social stratification, that leads to a new pattern of demand and form of consumption, but also to new needs, identities, forms of consensus and contradictions. If the changes in the supply side find a match in the changes developing on the demand side, the development of new technologies may offer a path of sustained growth for the economy, leading to a new cycle of accumulation (ibid.).

Once the 'technological paradigm' is established, a 'technological trajectory' develops, as decisions are made looking for the best possible trade-off between the variables characterizing the paradigm. The new outcomes are the result of the cumulative nature of technological change, the use of past experience, the patterns of market relations, government decisions, institutional pressures, social conflicts, (Dosi 1982; Nelson and Winter 1982).

In this context, the contrast between civilian and military goals is a long standing driver leading to a diversity of technological trajectories. Typically, civilian trajectories are market driven, constrained by the pressure for cost minimisation, wide applicability and mass consumption, and are shaped by competition among several oligopolistic players with a variety of capabilities. Conversely, military trajectories are shaped by requirements of the military with an emphasis on command and control, a focus on maximum performance requirements, with little attention to cost considerations and frequent economic inefficiencies. A detailed discussion of civilian and military technologis is in section 3 below.

All these processes unfold through market relations and political agency on an international scale; by their very nature, they transform the division of labour and countries’ position. National economies may find their previous specialization threatened, resulting in crises and decline. Countries’ political and military power can also be affected. Governments’ industrial and technological policies are key tools for attempting to shape the outcomes of technological change and reacting to such transformations.

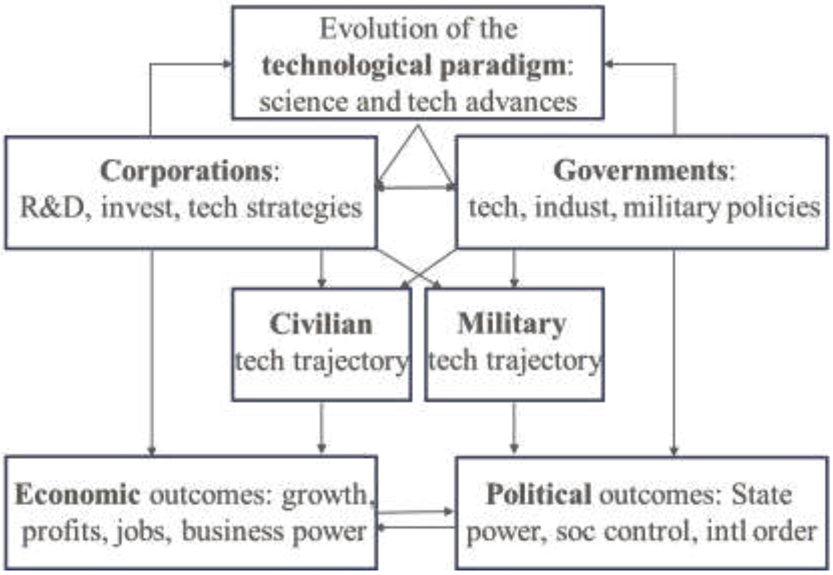
A political economy perspective is required in order to integrate in a coherent conceptual approach such diversity of issues – technological change, market processes, government policies, civilian and military goals. The approach that we adopt in this article is summarised in Figure 1. Within a given technological paradigm, corporations make decisions on the quantity and quality of their R&D, investment and production activities shaping their technological capabilities and strategies in the context of market dynamics. In parallel, governments develop technological and industrial policies – including military-related ones – with the goals of supporting the performance of national firms and of strengthening State power in domestic and international contexts.

The actions of corporations and governments shape the civilian or the military orientation of the trajectories of the current technology systems; there is a clear divide between the two in terms of performance or cost criteria, effectiveness of efficiency concerns, while, at the same time, there may be convergence in particular capabilities, strategies and programmes.

The outcomes of such processes can first be examined in economic terms – with the performances in terms of GDP growth, business profits and power, employment and distribution effects. Second, the outcomes can be assessed in political terms, with the evolution of State power in both the domestic context – the relationships with national firms, social consesus, political legitimacy – and in the international arena, with patterns in inter-State relations, power projection through military force, influence on the international order.

Within this conceptual framework, we will summarise in section 2 the characteristics and evolution of the digital technological paradigm, in section 3 the drivers of the divergence or convergence in the civilian and military trajectories in the digital age, in section 4 the strategies of US digital platforms and in section 5 the evolution of US military industrial and technology policy. The focus of the investigation will be the US – the leader in digital technologies.

Figure 1. The drivers of civilian and military technological trajectories


Evolution of the **technological paradigm**: science and tech advances
Corporations: R&D, invest, tech strategies
Governments: tech, indust, military policies
Civilian tech trajectory
Military tech trajectory
Economic outcomes: growth, profits, jobs, business power
Political outcomes: State power, soc control, intl order

2. The rise of digital technologies

A large literature has examined the characteristics of the ICT technological paradigm and of the current digital age. In this section, we focus on selected aspects that are relevant for understanding the patterns of civilian and military digital trajectories.

The technological paradigm based on ICTs that has emerged in the 1980s (Freeman and Louçã, 2001), had its roots in advances in the fields of microelectronics, computer science, communication and aerospace. The large US military procurement in aerospace and electronics of the 1960s and 1970s – associated to the construction of nuclear ballistic missiles, large mainframe computers and centralised control systems – contributed to such advances, with a close connection between civilian and military goals in the development of ICTs (O'Mara, 2020).

The ICT wave of the 1980s, however, was marked by a series of radical innovations including personal computers – breaking away from the previous model of IBM-dominated large computers -, communication systems – with the rise of mobile phones -, a network model of interactions – as opposed to the central control of previous large organisations -, and the Internet as a completely novel, decentralised infrastructure. The rapidly falling costs of computing and communication, the pervasiveness of their applications, the new possibilities they offered for control and coordination – for instance of global production networks – are at the root of the extension of ICT use throughout the economy and human activities. Such capabilities – in R&D, technology and production - have spread rapidly to other countries, in particular in East Asia – first in Japan and South Korea, then in Taiwan, Singapore and China – leading to complex international production networks also in advanced digital products.

All these factors have been associated to the dominance of a civilian trajectory for ICTs. However, military efforts were relevant in several cases. The Internet itself has military origins and was developed from Arpanet, a project overseen by the Pentagon's Advanced Research Projects Agency (ARPA) in partnership with researchers from West Coast universities (Stanford, UCLA, CalTech) (Mowery, 2010, O'Mara, 2020, Hawley, 2021). In the mid-1980s, another major US military initiative – the 'Star Wars' programme launched by US President Ronald Reagan in 1983 – introduced a challenge to the trajectory of high technology (see the next section).

Since the 1990s, ICT technologies have continued to evolve, with a major turn with the commercialisation of the Internet in the early 2000s (Greenstein, 2001) and their key role in the development of international production networks (Coveri et al., 2022). In the new century, the expansion of digital activites has led to the rise of large oligopolistic players, mainly in the US – the so-called 'Big Tech' including Alphabet, Amazon, Apple, Meta, Microsoft - and of the digital platform business model – discussed in section 4 below. This has been favoured by a complex combination of R&D, technology, industrial and regulatory policy in a neoliberal policy context. The balance of power between the State and corporations has tilted, with investment of large public resources, private control over technological outcomes and a growth of monopolistic power of large digital corporations. The pervasive nature of these developments and the global reach of their economic activities has shaped today's world economy.

US digital corporations have developed the digital platform business model, introducing important novelties, leading to what has been defined 'Surveillance capitalism' (Zuboff, 2019). The main players have built world monopoly positions in information-related activities, in key areas of human interaction, offering 'free' services to users but capturing systematic knowledge on their activities and behaviour. The logic of surveillance capitalism has become the extraction of all available information from individuals, the prediction and influence of their behaviour – as consumers, workers and citizens – the selling of this information to businesses tailoring their supply to specific consumer profiles, the organisation of global platforms where novel models of flexible work organisation can be developed (Kenney et al., 2021).

Data on individuals – habits, preferences, activities – have become a commodity that can be sold for a profit to advertisers and other business. The individualisation of communication and marketing for producing tailor-made consumption goods responding to needs reshaped by 'influencers' is a major novelty in the design of economic activities. The monopolistic power of digital platforms at the world level – and their ever extending activities in new fields of human interaction – is a major break with the idea of the importance of competitive markets and with traditional antitrust policies.

The financial dimension of such power is a further novelty. The profit potential of this model of capitalism has been promptly recognised by the financial system, leading to an extreme rise in the capitalisation value of major digital firms. In parallel, the actual production of goods and services – that requires the employment of workers - has taken second place, left to industries and countries outside the 'digital core' of the world economy.

These transformations are changing the nature of capitalism; but they also aim to constrain human nature, the freedom and ability to act, and represents a major challenge to democracy. Zuboff argues that "surveillance capitalism annexes human experience to the market dynamic so that it is reborn as behaviour" (ibid. p.514). Human experience becomes a new commodity shaping the new age of capitalism in the same way as – in Karl Polanyi's analysis (Polanyi 2001) - the transformation into commodities of land, labour and money were crucial for the rise of industrial capitalism.

The trajectory of digital technologies – largely shaped by civilian goals, market processes and individual activities – has been characterised by major advances in the capabilities of remote control, coordination, big data analysis, surveillance and targeting. They have been crucial for the ability of US digital platforms to reach their monopolistic power. And, in recent years, such qualities have increasingly been crucial for US military goals too. After a long phase of divergence, there are signs of a new convergence between civilian and military trajectories of digitalisation in the US.

Such developments have consolidated US digital leadership and the relevance of industrial and technology policy in these fields, with a further weakening of European digital capabilities. On the other hand, in the last decade China has emerged as the technological challenger of the US with the rise of its own digital platforms, comparable to the US ones.

In recent years, new security concerns (e.g., US-China rivalry, local wars, cyberwars) have emphasized the role of digital technologies in military strategies, both as a factor shaping global technological hierarchies and as a key component of frontier weapon systems. Military priorities and large defence-related procurement contracts are becoming a rapidly growing area of activity of major US digital corporations, with potentially relevant impacts on the evolution of the digital technological paradigm. Issues of surveillance, remote-control and autonomous systems, manipulation of information and social control are at the centre of new developments and may affect also the evolution of applications in commercial and public service domains. The implications for technology and industrial policy are wide ranging – with a particularly critical situation in Europe -, raising questions of public priorities, the balance of power between military and civilian interests and the risk of the emergence of a digital-military-industrial complex.

3. The relationships between civilian and military trajectories

The question of the relationships between civilian and military technologies is rooted in the broader debate on the contradictory nature and impact of the military economy. On the one hand, military expenditure acts as a 'Keynesian-style' stimulus to the economy through the increase of public demand, compensating problems of underconsumption and stabilizing the cycle of growth (Baran and Sweezy, 1968). They may also have positive supply-side effects by supporting R&D and new technologies, as in post-war US (Dunne and Tian, 2013).

On the other hand, for a given level of productive capacity, an increase in military expenditure may have negative effects on growth. Military activities may absorb a significant part of a country's limited capabilities in research, technology, human skills, capital accumulation and finance. In the case of the US, this has led to business practices that have inflated costs, prices and profits, and reduced efficiency (Melman, 1970,1974, Markusen, 1986). In a recent assessment of the impact of military expenditures on GDP and jobs in Europe, using an input-output model, the effect of investment in education, health and the environment has been found to be significantly greater than that of arms procurement (Stamegna et al., 2024).

In the case of technologies, a similar contradictory nature has long been identified (Pianta, 1988a). Military R&D is a major part of US innovative activities and technology policy. The positive effects of military research have been described as civilian 'spin-offs'. The negative effects include a distortion of research priorities and patterns of innovation; the concentration in military projects diverts resources - R&D funds, scientists, laboratories and production – away from the development of commercial technologies (Tirman, 1984). This concern has become greater with the rising power of East Asia in research and production of digital goods and services that the US is no longer able to produce.

The issue of civilian spin-offs is at the core of many studies on military programmes, from aircrafts to nuclear power, from semiconductors to computers (Smith, 1985). No general mechanism and pattern of technology transfer from military to civilian applications can be found, although institutional factors, funding for basic research, or procurement contracts at an early stage of development, played a role in the development of some of the new technologies. In the case of semiconductors, early procurement was the most important factor; in the early 1960s, the military accounted for half the total sales of semiconductors in the US, a share that fell to 10 per cent in 1981, and half of all the R&D has been paid for by the US Defense Department in this way (Flamm 1984: 36).

The lessons of this case, according to Rosenberg, are that "(1) The major innovations were not achieved on projects supported by military R&D. (2) Military R&D on possible alternative routes to miniaturization were largely spent 'betting on the wrong horses'. (3) The procurement needs of the military provided a pervasive and well-understood presence that served as a powerful inducement to innovative activity on the part of private firms spending their own R&D money" (Rosenberg, 1986: 18).

The case of nuclear power is an example of a highly unsuccessful technology on commercial terms that was developed from military research on nuclear weapons. Supersonic aviation is a failed attempt to use for commercial airlines technologies developed for military aircraft; the sixteen Franco-British Concorde airplanes that were produced had extremely high costs, while Boeing's SST project was never developed; the conclusion is that "the indiscriminate pursuit of military spillovers thus turned out to be a recipe for commercial disaster when optimal design requirements of the military and civilian sectors were sharply divergent" *(ibid.:* 24).

In the same vein, according to Nelson, the military and space programmes "surely do not provide us with a model for future policies in support of high technology industries. That US procurement and procurement-related R&D had such a strong effect in building commercial leadership of US firms certainly does not provide a persuasive argument that we should augment our present defense and space programmes to increase 'spillover.' The massive expenditures we mounted then, and are incurring now, surely cannot be justified by the commercial returns" (Nelson 1984a: 72).

The potential for spin-offs has also declined due to the falling importance of basic research within military R&D, to the lack of cost considerations in military programmes and to the divergent performance requirements of military and commercial projects.

In fact, the development of military technologies has an effect on the direction of technological change that goes beyond the simple diversion of resources from civilian innovation. A set of factors - basic principles, technological preferences, performance requirements, nature of demand - have a strong effect on the kind of technologies developed by the military, in ways that have reduced efficiency, slowed down civilian applications and distorted the overall direction of technical change.

The inefficiency of technological systems developed on the basis of military requirements, in the case of numerically controlled machine tools and nuclear reactors, has been shown by detailed reconstructions of their development and by international comparisons with the same technologies developed on other countries in a civilian environment (Tirman, 1984).

David Noble has documented how the development in the 1950s of numerically-controlled machine tools at the Massachusetts Institute of Technology with the funds of the US Air Force has led to machinery that offered a strong centralization of control and wide versatility, while ignoring cost constraints: "in an effort to meet Air Force specifications therefore, the industry ended up with perhaps the more complex and expensive approach to N/C (numerical control) then available" (Noble 1984: 203). Cost constraints have limited the use of such machines in US civilian industry, allowing Europe and Japan a later entry in such technologies with greater market success. Similar problematic outcomes have emerged in later years in industrial automation programmes sponsored by US armed forces with the goals of centralised control and a 'factory without workers' (Pianta, 1988a).

The extreme performance requirement and disregard for cost considerations have led Mary Kaldor to describe them as a 'baroque arsenal': "Modern military technology is not advanced; it is decadent. Over the years, more and more resources have been spent on perfecting the military technology of a previous era. As a consequence, modern armaments have become increasingly remote from military and economic reality. They are immensely sophisticated and elaborate; they are feats of tremendous ingenuity, talent and organization; and they can inflict unimaginable destruction. But they are incapable of achieving limited military objectives and they have successively eroded the economy of the United States and the economies of those countries that have followed in her wake" (Kaldor, 1982a: 1). Moreover, "baroque military technology artificially expands industries that would otherwise have contracted. It absorbs resources that might otherwise have been used for investment and innovation in newer, more dynamic industries. And it distorts concepts of what constitutes technical advance" *(ibid.: 3).*

How relevant are such arguments for the technologies developed in the context of the ICT paradigm? The relationships between civilian and military technologies in the 1980s are particularly interesting as they refer to the terminal phase of the military trajectory of the 'Fordist' technological paradigm - based on tanks, ship and aircrafts, the weapons of world war II – and the rise, at the same time, of the ICT technological paradigm. In the 1980s, a wide range of new technologies had emerged, including microelectronics, computers, telecommunications, space and new materials, that eventually become key elements of the new ICT paradigm. Other, separate fields of progress, included biotechnologies and genome research.

With the US presidency of Ronald Reagan, in the context of the New Cold War, a variety of industrial and technology policies were launched – with relevant responses from both Europe and Japan - attempting to shape the evolution of the new paradigm in a direction more favourable to the competences and interests of each area; detailed investigations are in Pianta (1988a, 1988b, 1988c). The emergence of the new ICT paradigm was a key theme of contention between alternative technological strategies, with a dramatic divide between military and civilian directions. Reinvestigating that episode – that shaped the making of digital technologies – is helpful to understand the current relationships between civilian and military technologies in the digital age.

In the 1980s the US had major industrial policies for microelectronics, fifth-generation computers, telecommunications,[†] as well as a policy of strict controls over the transfer – also from allied countries - of military-relevant technologies to the Soviet Union and other rival countries, enforced by the CoCom – the Coordinating Committee on Multilateral Export Controls that included NATO countries and Japan[‡] (Pianta, 1988a).

Most importantly, in 1983 the US launched the largest research programme ever financed by a Western government – the Strategic Defence Initiative, often referred to as 'Star Wars'. Funded with $33 billion over the 1984-90 period, the programme included research, development and testing of a new generation of high-technology weapons to be deployed in space and on earth, to defend the US from Soviet nuclear missiles, with the idea of making such weapons 'obsolete'.

In the military sphere, the development of high-technology weapons has always been at the core of the US military strategies aiming at superiority against rivals. In the Star Wars programme, however, a dominant role was taken by the major military aerospace industries of the time, the same companies that produce US nuclear weapons: the MX missile (Rockwell, TRW, Avco, Martin Marietta), the B-1 bomber (Rockwell, Avco, Boeing, LTV), the Pershing (Martin Marietta), the Trident (Lockheed), cruise missiles (Boeing, Litton). While US universities also obtained large research contracts, it is remarkable the absence of ICT corporations from the list of major SDI contractors (Pianta, 1988a, 1988b).

[†] In the 1980s, major US Defense Department programmes in ICT included the Strategic ccomputing programme and the Very high speed integrated circuis (VHSIC). Private sector cooperative efforts among majot ICT companies included the Microelectronics and Computer Technology Corporation (MCC) and the Semiconductor Research Corporation (SRC)
(Pianta, 1988b).

[‡] US and Japanese companies were threatened by US sanctions whenever they were trying to export to Soviet bloc countries goods in the Defense Department list of 'prohibited technologies, including military goods, machine tools, telephone switching equipment, personal computers, even if they were produced with mostly European technology.

In terms of the economic impact, the US government argued that the results of SDI research would have extensive applications in other areas, with the promise of a high-technology future for a US economy facing growing challenges from Europe and Japan. SDI represented an important attempt of the US to direct the future technological progress towards sophisticated military technologies. This is the area where the US has always had a remarkable advantage, putting under pressure the innovative strategies by the other advanced countries.[§]

It is important to note that in the 1980s, the policy responses from Europe and Japan distanced themselves from the military trajectory pursued by the US and emphasized civilian priorities. The European Community responded with a set of common research programmes mainly in civilian ICT areas: the 1987-91 'Framework Programme' of the European Commission, the Esprit programme in information technology and RACE in telecommunications. Another important French-initiated Europe-wide initiative, developed as a specific response to the US Strategic Defence initiative, was the Eureka programme, with a focus on ICT commercial technologies (Pianta 1988b). At the same time, the Japanese response to Star Wars included the Fifth-generation Computer Programme in ICTs as well as – in the field of biosciences and biotechnologies - the Frontier Reseacrh Programme and the Human frontiers science programme.[**]

At the onset of the digital age, competition and conflict over technological trajectories shaped for a decade the investment and policy efforts of the US, Europe and Japan. The eventual outcome was decided not by technological or military success, but by political developments. The rise to power of Michail Gorbacev in the Soviet Union opened the way to the end of the Cold War, a process of limited disarmament and the slowing down of the technological arms race. Star Wars were forgotten – after having spent very large funds on failed technological ideas - and the trajectory of the ICT technological paradigm took the road of civilian activities. The next section investigates developments within US digital corporations; section 5 will examine current US initiatives in military and digital technologies.

4. The power of US digital corporations

In contrast with the early days of the Internet, marked by the idea of decentralised networks of very large numbers of worldwide digital actors, offering innovation and economic opportunities to everyone (O'Mara, 2020), the evolution of digital technologies has seen the progressive consolidation of large US digital corporations. A key turning point was the US government decision in the mid-1990s to open up the 'commercialization' of the Internet (Greenstein, 2000), leading to an unprecedented concentration of techno-economic power (Rikap, 2021).

We focus here on the major US digital corporations – Alphabet (Google), Amazon, Apple, Meta and Microsoft. Their activities occupy the whole range of digital-related business, including hardware and software, phones and communication, big data management and cloud services, business support and retail sales, logistics and delivery, news media and social media, entertainment and movies, with major investment also in AI systems. Their growth in the last decades has been extremely rapid and Table 1 reports their market capitalization, revenues and profits in 2024 and 2025. In March 2025 their combined market capitalization is three times the GDP of Germany and not far from that of the entire Euro Area ($16 trillion). In 2024, their share of profits over revenues is at 27%, a very high value for US companies. R&D expenditure is 13% of revenue.

[§] As E. P. Thompson noted "Seen in this light, the aim of SDI is not to 'enhance deterrence,' but to enhance the competitiveness and technological supremacy of United States industry. It is a means of organizing research and development to the decisive advantage of the USA into the twenty-first century, so that both economic and security controls would ensure a one-way traffic" (Thompson 1985: 119)

[**] A detailed comparison of high technology programmes of the 1980s in the US, Europe and Japan is in Pianta (1988b).

Table 1. Alphabet, Amazon, Apple, Meta and Microsoft
Market capitalization, revenues, profits as a percentage on revenues and R&D

Corporations	Market capitalization March 2025 (US $ trillion)	Revenues 2024 (US $ billion)	Profits 2024 (% over total revenues)	R&D expend. 2024 (US $ billion)
Alphabet	2.05	350	29	49
Amazon	2.16	637	9	88 (incl. infrastructure)
Apple	3.58	391	24	31
Meta	1.65	164	38	43
Microsoft	2.89	245	36	29
Total	***12.33***	***1,787***	***27***	***240***

Source: authors' elaboration on Yahoo! finance and companies' investor declarations.
https://investor.atmeta.com/investor-news/press-release-details/2025/Meta-Reports-Fourth-Quarter-and-Full-Year-2024-Results/default.aspx; https://s2.q4cdn.com/299287126/files/doc_financials/2024/q4/AMZN-Q4-2024-Earnings-Release.pdf;
https://d18rn0p25nwr6d.cloudfront.net/CIK-0000320193/c87043b9-5d89-4717-9f49-c4f9663d0061.pdf;
https://abc.xyz/assets/77/51/9841ad5c4fbe85b4440c47a4df8d/goog-10-k-2024.pdf;
https://view.officeapps.live.com/op/view.aspx?src=https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/2024_Annual_Report

The evolution of digital technologies is now shaped by the power of such corporations. But what are the sources of their astonishing rise?

They have developed a *digital platform* business model that has combined a large number of unprecedented advantages (Kenney and Zysman, 2016; Rikap and Lundvall, 2021). Digital platforms are able to offer a wide range of services, some of them free to customers, addressing the whole range of economic, social and individual activities. By connecting as many applications as possible to the dominant platform, they have managed to extend their reach and lock-in users (Gawer and Cusumano, 2014). In their online interactions with them, digital platforms gather extensive and detailed data on habits, preferences, activities; they have become data-intensive surveillance-based businesses (Zuboff, 2019), increasing their ability to capitalise on network effects (Calvano and Polo, 2021) and winner-takes-all mechanisms (Gawer, 2022).

They have control over knowledge (Rikap, 2024), frontier technologies such as the Cloud and AI (Van der Vlist et al., 2024) and physical infrastructures such as data centres and submarine cables (Gjesvik, 2023). Their large market power allows them to lock-in customers (Jacobides et al., 2024) and influence their behaviour (Zuboff, 2019). 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).

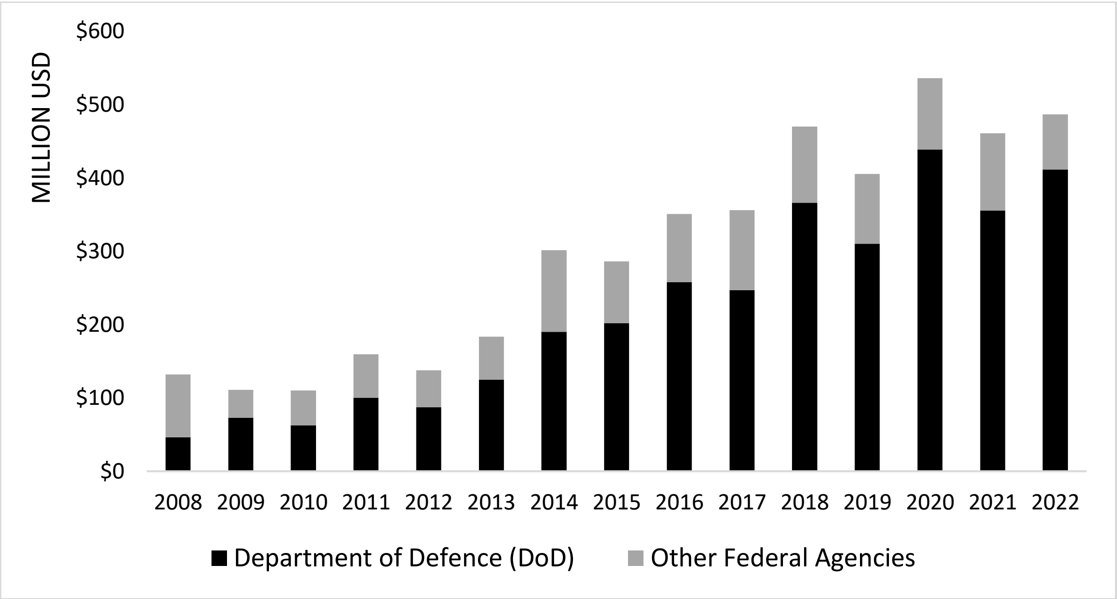
While the activities of US digital corporations have largely developed in commercial domains, some characteristics of their technologies – already pointed out in section 2 above - have made them relevant for warfare and intelligence activities too. They include key strengths in activities of remote control, coordination, big data analytics, surveillance and targeting. Moreover, their systemicinfrastructural nature (Kenney et al., 2021), and their control over a wide range of technologies, has made them an essential component of military activities (Coveri et al., 2022, 2024; Rikap, 2025). Control and coordination in battlefield operations now rely heavily on support services provided by US digital corporations (Gonzales, 2022). Some of these technologies in the area of communications are highly valuable for pursuing intelligence activities, ensure digital access in areas of conflict or where telecom infrastructures are lacking, carry out and prevent cyber-attacks (Farrell and Newman, 2023).

In the aftermath of the 9/11 attacks, US military and counter-terrorism policy recognised the value of the digital infrastructures and technologies – from data centres to machine learning algorithms – that was developing in US digital corporations (Farrel and Newman, 2022). New relationships were established, breaking with the original image of a Silicon Valley culture independent from the government and remote from the military-industrial complex (Lehdonvirta, 2022, Rikap, 2025).

A paradigmatic case is the georeferencing system developed by Alphabet (then Google) — Google Earth — which enables one of its most popular applications, Google Maps (Lee, 2010). Google Earth is the result of one of the first investments put forth by Q-Tel, a venture capital firm founded by the CIA in 1999 aimed at accessing the best start-ups. In this circumstance, the recipient was a San Francisco-based start-up, Keyhole, which developed the Google Earth's predecessor, EarthViewer. In 2004, Google acquired Keyhole for an undisclosed amount, revamped the software and, in 2005, launched Google Earth as one of its flagship innovations. After that, the relationship between Google and the military/intelligence apparatus becomes increasingly close, particularly regarding technologies aimed at managing and interpreting satellite imagery (Gonzales, 2022).

A key indicator of this growing relationship is the number and amount of procurement contracts focused on intelligence or military activities, awarded to US digital corporations by the Department of Defense (DoD), the CIA, the NSA, the Department of Justice and related agencies. Focusing on Alphabet, Amazon, Meta and Microsoft, Coveri et al. (2024) documented that, from 2007 to 2022, military and intelligence-related procurement contracts grow at a rate of about 200 per year. Figure 1 reports the value of procurement contracts awarded to these companies between 2008 and 2022, highlighting the share of resources stemming from the DoD.

Figure 2. US Federal procurement contracts awarded to Alphabet, Amazon, Meta and Microsoft, 2008-2022



Source: adaptation from Coveri et al. (2024)

Table 2. US Military contracts to digital corporations
Selected military contracts from the the Department of Defense, the CIA and the National Security Agency to US digital corporations (2013-2024)

Year and Dept.	Contractor	Amount ($ million)	Nature of activities	Stated objective
2013 – CIA	Amazon	600	Cloud	Data management for preventing terrorist attacks
2019 – DoD Project Maven	Alphabet (withdrawn); Amazon, Microsoft	50	Drones	Acquisition of AI technologies for reconnaissance of images from military drones
2020 – CIA Commercial Cloud Enterprise C2E	Alphabet, Amazon, Microsoft, Oracle	Tens of billion	Cloud	Cloud services for 17 intelligence agencies
2021 – DoD HoloLens	Microsoft	21,900	Visors and augmented reality	HoloLens augmented reality headsets for military activities in highly complex environments
2022 – NSA Wild and Stormy project	Amazon	10,000	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	9,000	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

Source: adaptation from Coveri et al. (2024)

Compared to the total revenues of US digital corporations, the value of such military and security-related contracts is rather small, although numbers could be underestimated due to the classified nature of military and intelligence-related contracts (Gonzales, 2022). What matters most, however, is the critical nature of the infrastructure, technology, and information that US digital corporations manage also for military and security purposes. Important insights can be obtained by Table 2 that reports a selection of contracts procured by the DoD, the CIA and the NSA to major US digital companies, highlighting amount, nature of the service and aims to be pursued in the military or intelligence domain.

Being in charge of data centres, cloud, submarine cables, AI systems aimed at preventing cyber-attacks or infrastructures used to ensure connectivity in areas of conflict, turns US digital corporations into the 'eyes and ears' of their government, both at home and abroad. They obtain access to critical information and develop unique competences; this puts them in a position of unprecedented strength in relation to the government, and their power can hardly be challenged by public policies with different goals (e.g., antitrust regulations).

Finally, in recent years the military role of US digital corporations has been further consolidated by their direct involvement in warfare activities. Three main cases have been documented. First, in the US war in Afghanistan, US digital corporations provided critical technologies for the target detection, recognition and autonomous weapons management (Gonzales, 2022).

Second, in the Ukraine war, US digital corporations are active on the ground in order to provide satellite-based Internet services used by the Ukrainian army rely to carry out its operations (with SpaceX); cloud services aimed at archiving and managing government and financial information (Amazon Web Services); dedicated platforms shielding government and financial institutions from Russian cyberattacks and allowing to manage energy grids, even in war zones (Microsoft) (Coveri et al., 2024).[††]

Third, in the Israeli war in Gaza, companies such as Alphabet and Amazon are key providers of AI-powered surveillance and targeting systems, used to carry out air strikes and military attacks.[‡‡] Palantir, a Silicon Valley company funded in the early 2000s and focusing on surveillance and military-related technologies, has developed a strategic partnership with the Israeli Defense Ministry, supplying AI tools to support the country's war.[§§]

[††] https://time.com/6691662/ai-ukraine-war-palantir/

[‡‡] https://www.business-humanrights.org/en/latest-news/ap-exposes-big-tech-ai-systems-direct-role-in-warfare-amid-israels-war-in-gaza/

[§§] According to *Bloomberg*, an agreement has been signed in January 2024 during a meeting between Israeli defense officials and Palantir co-founders Peter Thiel and Alex Karp in Tel Aviv. https://www.palantir.com/assets/xrfr7uokpv1b/3MuEeA8MLbLDAyxixTsiIe/9e4a11a7fb058554a8a1e3cd83e31c09/C134184_finaleprint.pdf [Last access: 6 March 2025)].

According to the Israeli journal *+972 Magazine*, "On Dec. 10 [2024], Israeli military officials, weapons manufacturers, and American venture capitalists gathered at Tel Aviv University for the first ever DefenseTech Summit. The two day affair featured panels on "The Future of Global Conflict," "Challenges of Iron Swords" (the Israeli army's name for the war in Gaza), and "Exploring Innovation in Drone Technology." Representatives from Palantir, Sequoia Capital, and Elbit shared the stage with the director-general of Israel's Defense Ministry and the head of "Lotem," the army unit devoted to big data and AI. Officially, the DefenseTech Summit was meant to showcase "Israel's cutting edge technologies and strategies for addressing global security." But the event felt more like a celebration of a new and unrestrained era of techno-militarization inaugurated by Donald Trump's re-election. As Palantir's Noam Perski put it in his speech on Tuesday morning, "All these people who used to be tech bros are now defense tech bros." S. Goodfriend, With Gaza war and Trump's return, Silicon Valley embraces a military renaissance. +972 Magazine, 31 December 2024, https://www.972mag.com/gaza-war-trump-silicon-valley-military/ [Last access: 8 march 2025].

According to *The Nation*, "As one of the world's most advanced data-mining companies, with ties to the CIA, Palantir's "work" was supplying Israel's military and intelligence agencies with advanced and powerful targeting capabilities. The project involved selling the ministry an Artificial Intelligence Platform that uses reams of classified intelligence reports to make life-or-death determinations about which targets to attack". J. Bamford (2024) How US Intelligence and an American Company Feed Israel's Killing Machine in Gaza, The Nation, 12 April 2024, https://www.thenation.com/article/world/nsa-palantir-israel-gaza-ai/ [Last access: 8 March 2025].

An additional indicator of the closer relationships between US digital corporations and the US military is the extent of the 'revolving doors' through which business managers move to occupy top government appointments and viceversa (Coveri et al., 2024). 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).

On the other hand, government officials and policy makers may bring to digital corporations an insider knowledge of the functioning of US agencies, of the evolution of legislation and regulation, of the programmes and contracts that are launched in military areas. Such insider information is crucial in areas – i.e., digital technologies – with a rapid pace of innovation and a lack of established regulatory frameworks.

Examples of moves from business to government include Doug Beck, former vice-president of Apple, recently appointed as the new director of the Defense Innovation Unit (DIU, see the next section). Another relevant case is Eric Schmidt, former CEO of Alphabet; together with former Secretary of State Henry Kissinger and ex-Deputy of Defense Secretary Robert Work, Schmidt has served as chairman of the Defense Innovation Advisory (DIA) Board and co-chairman of the National Security Commission on AI (NSCAI), two government advisory boards aimed at accelerating DoD's technological innovation programmes countering the emerging technological power of China. At the same time, Schmidt relied on his own venture capital to invest in defence start-ups, thus becoming an important actor on 'both sides of the table'.[***]

Examples of moves from government to business include Josh Marcuse, who was executive director of the Defense Innovation Advisory (DIA) Board since 2016, and in 2020 became head of strategy and innovation for Google Public Sector, the division developing technologies for public institutions, including the military. In advising the Department of Defense, Marcuse was an early advocate for the Joint Enterprise Defense Infrastructure (JEDI) cloud contract[†††] and played a key role in shaping the ethical guidelines for the Joint Artificial Intelligence Center of the US military.

Besides developing technologies relevant for military objectives and receiving Federal contracts, US digital corporations have also developed close relationships with the US government in the context of policy making and regulations. A major priority of firms has been avoiding government actions in the areas of anti-trust policy, protection of data and privacy, taxation of digital activities, limitations to business activities; at the same time the government has become an increasingly important customer for the sale of digital services (O'Mara, 2020; Rolf and Schindler, 2023).

Relationships with the US government were also essential for making the expansion into foreign markets possible, using US power in order to force foreign governments to accept the unfettered operation of US digital corporations in their economies and societies (Kwet, 2019).

The policy making of the US government that has been relevant for shaping digital technologies and relationships with major US corporations is examined in the next section.

[***] On this point, see: Conger, K., and Metz, C., '"I Could Solve Most of Your Problems": Eric Schmidt's Pentagon Offensive', The New York Times, May 2, 2020 (Updated Nov. 3, 2021), available at: ttps://www.nytimes.com/2020/05/02/ technology/eric-schmidt-pentagon-google.html. See also Javers, E., 'How Google's former CEO Eric Schmidt helped write A.I. laws in Washington without publicly disclosing investments in A.I. startups", CNBC, 24 October 2022, available at: https://www.cnbc.com/2022/10/24/how-googles-former-ceo-eric-schmidt-helped-write-ai-laws-in-washington- without-publicly-disclosing-investments-in-ai-start-ups.html. Last access: 8 September 2023.

[†††] The JEDI was a large cloud computing contract which has been reported as being worth $10 billion. After a controversy, the contract has been awarded to Microsoft in 2019 but then halted in 2021. It has been further transformed in the JWCC and awarded to Alphabet, Amazon, Microsoft and Oracle (see Table 2).

5. US industrial and innovation policies for the militarization of digital technologies

As US digital corporations were moving closer to military capabilities, industrial and technology policies of the US government became a novel driver for the convergence of military and civilian trajectories. We focus on three key policies: first, the overall R&D, technology and arms procurement programmes of the Department of Defense (DoD); second, the evolution of DARPA as the major player in the development of military high technology; third the new role of the Defense Innovation Unit (DIU) as the key actor in the ecosystem of smaller US digital firms involved in military activities.

The Department of Defense

The budget of the DoD is the major source of funds for US military activities. In the FY 2024 budget, the DoD has requested $315 billion in weapon systems acquisition funds, up from $276 billion in 2023. Of this total, $170 billion is allocated for procurement and $145 billion for Research, Development, Test, and Evaluation (R&DTE). Digital technologies dominate the R&D efforts, with major increases in cyberspace, spectrum, AI, 5G, and other digital-related programmes (DoD, 2024). Additional information comes from the DoD Weapons Acquisition Programme (WAP) (DoD, 2025a). The overall funding request for 2025 totals $310.7 billion, including $167.5 billion for procurement and $143 billion for R&DTE.

Funding for 'Command, Control, Communications, Computers, and Intelligence' (C4I) – a mission dominated by digital technologies – went from $7.4 billion in 2017 to $12.8 billion in 2023 and to $21 billion in 2025, showing the fastest rise among DoD budget components. It includes command centres, data processing and other information technology, communications systems, air traffic control, night vision equipment, cyberspace activities.

Funds for Science and Technology (S&T) activities amount to $18 billion in 2025, and the WAP priorities include: applications of AI and Machine Learning, 5G, microelectronics, quantum sciences, cyberwars, hypersonics, directed energy weapons (lasers, particle beams, etc.), biological technology, and space.

The amount of annual US government expenditure in digital-related military technologies – including R&D, arms procurement and systems management – is hard to identify but, based on the above data, could possibly be in the range of about $ 100 billion, an order of magnitude that could effectively shape the trajectory of digital technologies. In Table 1 we have seen that in 2024 the total R&D expenditure of the top five US digital corporations was $240 billion. This amount includes the military R&D contracts received by these companies; such data suggest that in many areas of digital research, the importance of the military is weighting heavily on the overall innovative efforts of digital corporations.

More specific insights on the militarization of digital technologies can be obtained from the analysis of the DoD Strategic Management Plan (SMP) 2022-2026 (DoD, 2025b). It emphasises "critical technology areas" considered vital "to address the key national security challenges the nation faces, including the Department's pacing challenge, the People's Republic of China" (DoD, 2025b p. 44). The Plan identifies, first, "areas of emerging opportunity", including biotechnology, quantum science, future-generation wireless, and advanced materials. Second, areas of "effective adoption", domains where there is "vibrant existing commercial activity", such as AI, autonomous vehicles, integrated networks, systems-of-systems, microelectronics, renewable energy generation and storage, advanced computing and software, and human-machine interfaces. The third area concerns defense-specific domains, including directed energy, hypersonics, integrated sensing and cyber. Digital models and simulations are considered to be crucial for combat capabilities, but also in the exploration of the most effective technologies to be developed (DoD, 2025b).

Special attention is devoted to Big Data, cloud infrastructures satellite communications and AI, deemed essential to manage and ensure the resilience of Command, control and communication systems. The DoD Plan argues that AI is "spanning the entire DoD mission space, including joint command and control, biotechnology, cyber, intelligence, information operations, space, and business operations" and is key to achieve autonomous decision making and continuous adversarial testing as well as neuromorphic systems aimed at emulating brain processes for decision-making on the battlefield (DoD, 2025b p. 96).

The military strategy for AI was at the centre of previous US policy documents - the DoD AI Strategy (2018), the DoD Digital Modernization Strategy (2019), the DoD Data Strategy (2020) – leading to the DoD Data, Analytics and Artificial Intelligence Adoption (DAAI) strategy (DoD, 2023) that emphasises the essential role of AI in effective decision making. According to this DoD strategic document, "fielding data, analytics, and AI capabilities from the boardroom to the battlefield (…) is key to address a broader array of operational problems, dynamically campaign and deter, and prevail in conflict" (p. 8).

In this context, data infrastructures assume a crucial role. The DoD Plan (2025b) reports a concentration of its infrastructures into few major data centers (54 out of 61 data centers have been closed) in order to increase efficiency and ease interoperability, and outlines a new interoperable federated infrastructure to promote semi-autonomous data collection and sharing.

As shown in Table 1 above, US digital corporations received major contracts for Big-Data management, cloud services and data infrastructures; the US military appears to heavily rely on private companies for a crucial part of its activities, bringing them closer to the military requirements and goals in digital technologies.

Closer interactions between the US military and digital corporations – including smaller firms and start-ups – are now a policy priority. In the case of Big-Data and AI, the DoD strategy emphasises that the effectiveness of technologies is related to the scale of the database used to feed the underlying algorithms, and suggests to remove bureaucratic barriers, easing data integration and transferability (DoD, 2023). The DoD Strategic Management Plan argues for a "blurring the organizational boundaries", allowing for "greater integration with technology developers", including increasing diffusion of data analytics and procedures that value data 'as-a-product', just as it happens in the commercial domain (DoD, 2025b, pp. 9-10). It quotes former Under Secretary of Defense for Research and Engineering Heidi Shyu: "as seen in Ukraine, novel commercial technology, paired with conventional weapons, can change the nature of conflict (…) The DoD's processes, ranging from programming, to experimentation, to collaboration, should be updated to redirect the dynamic landscape of today and anticipate the needs of tomorrow' (DoD, 2025a, p. 95).

Greater relationships with a large number of digital companies would favour – in the US military strategy – learning processes and access to advanced civilian systems with dual-use – both civilian and military – potential. The DoD Plan aims to "engage commercial companies to identify opportunities in order to leverage their dual-use technologies for military applications" (DoD, 2025a, p. 95). The list of US military agencies and programmes that have such a task includes the DIU (see below), US Air Force's AFWERX, US Navy's NavalX, US Army's Rapid Capabilities and Critical Technologies Office, US Army's XTECH, US Special Operations Command's SOFWERX, US Space Force's WERX.

A further reason for the US military interest in digital corporations is the acknowledgement of a lack of the skills associated to critical technologies. In the DoD Plan, Strategic priority 4 states that "to create 21st century capabilities, the most talented people in the world is needed" (DoD, 2025b) and, in spite of efforts to expand hiring in the military, US digital corporations are still the place where top talents are currently found.

The evolution of DARPA

In shaping new technologies, at the crossroads between military and civilian directions, a key role has long been played by DARPA – the Defense Advanced Research Project Agency of the Defense Department.

Established in 1958, after the ‘Sputnik shock’, DARPA’s task was to close the gap in aerospace technologies and, more broadly, to achieve innovation-related ‘missions’ characterized by radical uncertainty and requiring costly and lengthy exploration efforts (Bonvillian et al., 2019). DARPA’s funding programmes, on the hand, encouraged basic research in cooperation with universities and R&D institutions and, on the other hand, favoured the transfer of scientific advancements into new military systems or civilian marketable innovations.

DARPA's technological priorities show a continuing evolution. Fuchs (2010) shows that they shifted from a focus in the 1970s on military-oriented S&T missions, to concerns on industrial competitiveness, microelectronics and dual-use technologies in the 1980s, to greater cooperation with universities in basic R&D in the 1990s, and finally, since 2001, focusing on dual-use digital technologies and on technology transfer from commercial to military applications. DARPA was also key player in the establishment of the Internet, contributing to interoperable network technologies that sped-up its commercialization (Greenstein, 2001) and the rise of US digital corporations examined in the previous section (Mazzucato, 2011). One of the recent outcomes of DARPA-sponsored research is the development of the voice-AI assistant named ‘SIRI’.

Operating as a ‘bridge’ connecting scientific advancements, technological opportunities and military needs, DARPA has close links with the large US digital corporations, encouraging the integration of smaller firms and start-ups into a broad ecosystem of digital innovation with dual-use potential.

DARPA's 2025 funding request to the US Congress highlight technological priorities and current trends (DoD, 2025d). The total funding request for 2025 amounts to 4.37 billion dollars, to be allocated to a variety of research programmes. Concerning basic research, the strongest growth in funding, between 2024 and 2025, is found in ICT (+20%) and biomedical technology (+20%). When it comes to applied research, the only areas displaying an increase in funding are related to the digital domain: space programs (+67%), command, control and communication systems (+5%), advanced electronics (+2%), and network-centric technologies (+1%). Among its ongoing projects, AI technologies play a prominent role, including human-machine teams, AI reasoning, and highly autonomous AIs.

One of the programmes – with a $41 million request for 2025 (twice the 2024 value) – is the Air Intelligence Reinforcements (AIR) – addressed to Air force pilots, aiming to “automate tactical control tasks transforming junior pilots from low-level tacticians into high-level mission commanders (…) while for unpiloted platforms, AIR will enable vehicles to perform missions with minimal human oversight” (DoD, 2025d p.182).

The Rapid Experimental Missionized Autonomy (REMA) – with a $13.8 million request, up from a $5 million in 2024 - aims at increasing the autonomous decision-making capabilities of drones developing dedicated software and digital tools (p. 183). A related programme, the Autonomy Standards and Ideals with Military Operational Values (ASIMOV) – with a request of $22 million, up from $5 million in 2024 - regards testing and maintenance software aimed at ensuring that autonomous weapons adhere to the DoD’s safety and ethics principles, particularly when such weapons are used in complex scenarios involving ‘ethical decisions’ (p. 220).

A key research area concerns human-machine interaction, or “symbiosis,” as DARPA calls it. The ACCESS programme – with a $13 million request - aims at making AI chatbots capable of realistic and positive dialogue; one of the objectives is to design large pre-trained generative AI models supplemented with legal sources to propose legal actions capable to deter adversaries. Another project – with a $9.5 million request – focuses on generative AI and studies how to increase AI capabilities to pursue abstract reasoning and to develop techniques enabling transparent and logical communications between humans and AI models (pp. 69-70).

In the current operation of DARPA, its long-term focus on digital technologies has led to novel priorities on AI-related opportunities. Its long-standing cooperation with business is now focused on US digital corporations and their networks of innovators and start-ups. Its traditional attention to dual-use technologies appears to be now a major driver of a convergence between the civilian and military trajectories of digital technologies.

The Defense Innovation Unit

The Defense Innovation Unit (DIU) - launched in 2015 by then Secretary of Defense Ash Carter[‡‡‡] - is a new US agency with the task to engage digital corporations in the development of defense projects, reducing the gap between the military and frontier commercial technologies; it operates as a liaison from "DoD and warfighter needs" to "tech sector creative minds that can solve the problem" (Harper, 2020 p. 2). Its headquarter is in Mountain View, in the heart of Silicon Valley; the first Director has been Eric Schmidt, former CEO of Google/Alphabet; the current Director, Doug Beck, has been Apple's Vice President between 2009 and 2023, in charge of business in the Americas and North-Eastern Asia.

Through R&D procurement and outsourcing of technological solutions for military needs, the DIU aims to build a close relationships with the major digital corporations, as well as with the constellation of firms relying on their platforms (Gawer and Cusumano, 2014). It encourages the emergence of new defense start-ups, accelerates the transition from prototypes to production of digital technologies for security systems and the battlefield and promotes the scalability of DIU-developed technologies across the various DoD segments (Jacobides et al., 2024).

A key concern of DIU is to operate like a commercial venture; it has the authority to enter into transaction agreements with private firms without the bureaucratic procedures of the DoD acquisition process. It is also expected to stimulate venture capital funding of new projects of military relevance. The DIU's top five technology areas are AI and Machine Learning, autonomous weapons, human systems, space, cybersecurity. In the area of AI, the DIU cooperates with the DoD's Chief Digital and Artificial Intelligence Office (CDAO) aiming to "leverage a unique cadre of 'dual fluency' talent and deep partnership with the warfighter to help bring the capabilities of commercial and nontraditional vendors to bear on the most critical needs those warfighters have".[§§§] The CDAO, on the other hand, ensures that the DoD data needed to exploit the potential of AI and related technologies can be safely used via CDAO-managed infrastructure, assuring compliance with standards and security protocols.

Finally, the DIU is also in charge of overseeing the National Security Innovation Network (NSIN), which includes universities collaborating with the DoD. Through its extensive contacts with Silicon Valley business and research institutions, and its focus on attracting frontier innovators to defense projects, the DIU is now a key actor shaping the military trajectory in digital technologies.

6. Towards a digital-military-industrial complex

We can now pull together the evidence from the emergence of the digital technological paradigm, the rise of US corporations along a mainly civilian trajectory, and the US industrial and technology policies in the defense area that are shaping a digital military trajectory.

Figure 3 summarises the evidence we have provided. Within the digital paradigm, the rise of US digital corporations has led to the platform business model characterised by monopoly power, management of Big Data and major capabilities of control, surveillance and targeting. Such a model has evolved along a civilian trajectory that has introduced major novelties in the economic system and in the technological landscape.

In parallel, government's industrial and technology policy has focused on 'strategic technologies' mainly in the digital field that are expected to provide major political and military advantages. We have found that the key characteristics of the civilian trajectory have become of major interest for

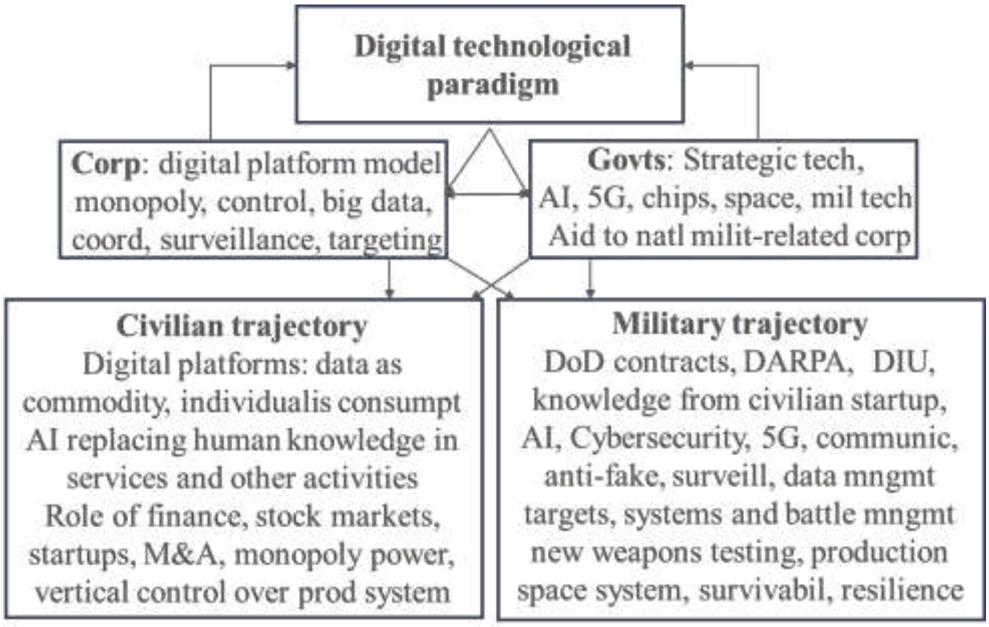
[‡‡‡] https://www.diu.mil/

[§§§] https://www.diu.mil/latest/diu-and-cdao-deploying-ai-for-strategic-impact military priorities; Big Data, remote control, surveillance and targeting are becoming the backbone of new modes of warfare.

Our analysis of US policy – with the cases of the DoD, DARPA and DIU – has documented the growing involvement of US digital corporations in defense activities, and the new convergence between civilian and military digital technologies. We have shown that the amount of military R&D and procurement in a variety of digital activities is now able to influence the overall evolution of technologies, tilting the balance between civilian and defense priorities.

Considering DoD strategies, the implementation of US industrial and technology policies in the defense field, and the efforts for an ever-closer integration between major corporations and security priorities, what we are witnessing is in fact the emergence of a *digital-military-industrial complex.* This represents a major novelty in a digital age that had grown out of a civilian trajectory.

Figure 3. Digital technologies: civilian vs military trajectories in the US


Digital technological paradigm
Corp: digital platform model monopoly, control, big data, coord, surveillance, targeting
Govts: Strategic tech, AI, 5G, chips, space, mil tech Aid to natl milit-related corp
Civilian trajectory
Digital platforms: data as commodity, individualis consumpt AI replacing human knowledge in services and other activities Role of finance, stock markets, startups, M&A, monopoly power, vertical control over prod system
Military trajectory
DoD contracts, DARPA, DIU, knowledge from civilian startup, AI, Cybersecurity, 5G, communic, anti-fake, surveill, data mngmt targets, systems and battle mngmt new weapons testing, production space system, survivabil, resilience

The expanding role of the military trajectory is affecting frontier research in crucial areas, including AI. In an essay published by the conservative Hoover Institution in December 2024, Eric Schmidt – the former CEO of Google/Alphabet – coauthored a policy document charting the trajectory of links between the US military and US digital corporations in the field of AI research: "[AI] threat evaluation requires a major effort that goes well beyond what governments are doing now (...) will require work with the most advanced models that we have made or that others could make (...) Governments now do not have the technical teams or the infrastructure to do this work (…). Frontier AI capabilities will become part of the defense industrial base of the free world, indispensable in evaluating dangers and developing countermeasures (...) governments will have to rely on the private sector to help build up the most advanced capabilities in the world, so that governments can then access, supplement, train, or fine-tune those capabilities to defend against dangers that may go beyond anything the companies conceive for their own private purposes (…) We must get started building the base camp (...), the next stage of relations between governments and industry at the AI frontier (…). If governments help sustain the companies essential to their defensive work, they may ask companies to accept certain obligations to protect the public interest" (Zelikow et al., 2024).

These developments represent a deep change in the evolution of our digital age, with far-reaching consequences. The question of the civilian vs. military trajectory in digital technologies – and in frontier areas such as AI – has now become an important policy question, calling for an informed public debate on the priorities for our society in the development of digital technologies, on the power of large corporations and on the goals of national policies.

References

Alic, J. (2007). Trillions for military technology: how the Pentagon innovates and why it costs so much. Springer.

Alic, J. A. (2008). A weakness in diffusion: US technology and science policy after World War II. Technology in Society, 30(1), 17-29.

Alic, J. A. (2014). The Origin and Nature of the US "Military-Industrial Complex". Vulcan, 2(1), 63-97.

Baran, P. and P. Sweezy (1968) *Monopoly Capital: An Essay on the American Economic and Social Order.* Harmondsworth: Penguin.

Bonvillian, W. B., Van Atta, R., & Windham, P. (2019). The DARPA model for transformative technologies: perspectives on the US defense advanced research projects agency (p. 510). Open Book Publishers.

Cartwright, M. (2020). Internationalising state power through the internet: Google, Huawei and geopolitical struggle. Internet Policy Review, 9(3), 1-18.

Coveri, A., Cozza, C., & 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., & Guarascio, D. (2024). Blurring boundaries: an analysis of the digital platforms-military nexus. Review of Political Economy, 1-32.

Cox, A. G., Moore, N. Y., & Grammich, C. A. (2014). Identifying and eliminating barriers faced by nontraditional Department of Defense suppliers.

Calvo, A. G., Kenney, M., & Zysman, J. (2024). Responding to platform firm power: differing national responses. New Political Economy, 1-15.

DoD (2023) Department of Defense Data, Analytics, and Artificial Intelligence Adoption Strategy Accelerating Decision Advantage Available at: https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF

DoD (2024) Defense Budget Overview FISCAL YEAR 2024 Available at: https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2024/FY2024_Budget_Request_Overview_Book.pdf

DoD (2025a) Department of Defense Program Acquisition Cost by Weapon System Fiscal Year 2024, Available at: https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2024/FY2024_Weapons.pdf

DoD (2025b) Department of Defense Strategic Management Plan Fiscal Years 2022 – 2026, Available at: https://media.defense.gov/2023/Mar/13/2003178168/-1/-1/1/DOD-STRATEGIC-MGMT-PLAN-2023.PDF

DoD (2025d) Defense Advanced Research Projects Agency Justification Book Volume 1 of 5 Research, Development, Test & Evaluation, Available at: https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2025/budget_justification/pdfs/03_RDT_and_E/RDTE_Vol1_DARPA_MasterJustificationBook_PB_2025.pdf

Dosi, G. 1982. "Technological paradigms and technological trajectories. A suggested interpretation of the determinants and directions of technical change". *Research Policy* 11 (3): 147-162.

Dosi, G., Freeman, C., Nelson, R., Silverberg G. and Soete L. (eds) (1988) Technical Change and Economic Theory, London, Pinter

Dunne, J. P., and Tian, N. (2013) "Military Expenditure and Economic Growth: A Survey." *The Economics of Peace and Security Journal* 8 (1): 5-11

Ergas, H. (1986) *Does Technology Policy Matter?* Brussels: Centre for European Policy Studies.

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

Flamm, K. (1984) Technology policy in international perspective. *In Policies for Industrial Growth in a Competitive World,* Joint Economic Committee, US Congress, 27 April.

Freeman, C. and Louçã, F. (2001) As time goes by. From the industrial revolution to the information revolution. Oxford, Oxford University Press

Freeman, C. and Perez, C. (1988) Structural crises of adjustment, business cycles and investment behaviour, in Dosi at al. (1988), pp.38-66.

Fuchs, E. R. (2010). Rethinking the role of the state in technology development: DARPA and the case for embedded network governance. Research Policy, 39(9), 1133-1147.

Gawer, A. (2022). Digital Platforms and Ecosystems: Remarks on the Dominant Organizational Forms of the Digital age. Innovation 24 (1): 110–124.

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

González, R. J. (2022). War virtually: The Quest to automate conflict, militarize data, and predict the future. Univ of California Press.

Greenstein, S. (2000). Building and delivering the virtual world: commercializing services for Internet access. The Journal of Industrial Economics, 48(4), 391-411.

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

Hawley, J. (2021). The tyranny of big tech. Simon and Schuster.

Kaldor, M. (1982a) *The Baroque Arsenal.* London: Deutsch, Abacus.

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

Kenney, M., Bearson, D., & Zysman, J. (2021). The platform economy matures: Measuring pervasiveness and exploring power. Socio-economic review, 19(4), 1451-1483.

Kuhn, T. S. (1962). The structure of scientific revolutions. Chicago: University of Chicago Press.

Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. Race & Class, 60(4), 3-26

Lee, M. (2010). A political economic critique of Google Maps and Google Earth. Information, Communication & Society, 13(6), 909-928.

Lehdonvirta, V. (2022). Cloud empires: How digital platforms are overtaking the state and how we can regain control. Mit press.

Lundvall, B-Å, and C. Rikap. 2022. 'China's Catching-up in Artificial Intelligence Seen as a co-Evolution of Corporate and National Innovation Systems.' Research Policy 51 (1): 104395.

Markusen, A. (1986) The militarized economy. *World Policy Journal,* Summer.

Mell, P. (2002). Big Brother at the door: Balancing national security with privacy under the USA Patriot Act., Denv. UL Rev., 80, 375.

Melman, S. *(1970) Pentagon Capitalism: The Political Economy of war.* New York: St Martin's Press.

Melman, S. (1974) *The Permanent War Economy: American Capitalism in Decline.* New York: Touchstone, Simon & Schuster.

Mowery, D. C. 2009. 'National Security and National Innovation Systems.' Journal of Technology Transfer 34 (5): 455–473.

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.

Nelson, R. (1984a) *High Technology Policies: A Five-Nations Comparison.* Washington, DC: American Enterprise Institute.

Nelson, R. and Winter, S. (1982), An Evolutionary Theory of Economic Change, Cambridge (Mass.), The Belknap Press of Harvard University Press

Noble, D. (1984) Forces of Production: A Social History of Industrial Automation, New York, Knopf.

Noble, D. (1985) Command performance: a perspective on military enterprise and technological change. In M.R. Smith (1985).

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

Perez, C. (1983), Structural change and the assimilation of new technologies in the economic and social systems, Futures, 15, 5, 357-75

Perez, C. (2002): "Technological revolutions and financial capital", Cheltenham, Edward Elgar.

Pianta, M. (1988a) New technologies across the Atlantic: US leadership or European autonomy? Hemel Hempstead, Harvester Wheatsheaf and United Nations University.

Pianta, M. (1988b) High Technology Programmes: for the military or for the economy? *Bulletin of Peace Proposals* 19,1.

Pianta, M. (1988c) Star wars as tech wars, Socialist Review, 18, 3, pp.83-102.

Pianta, M. (2019) Technology and Work: Key Stylized Facts for the Digital Age. In K. F. Zimmermann (ed.), Handbook of Labor, Human Resources and Population Economics, Springer, https://link.springer.com/referenceworkentry/10.1007/978-3-319-57365-6_3-1

Polanyi, K. (2001) The Great Transformation: The Political and Economic Origins of Our Time, Boston, Beacon Press (original edn 1944).

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

Rikap, C. (2024). Varieties of corporate innovation systems and their interplay with global and national systems: Amazon, Facebook, Google and Microsoft’s strategies to produce and appropriate artificial intelligence. Review of International Political Economy, 31(6), 1735-1763.

Rolf, S., & 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.

Rosenberg, N. (1982) *Inside the Black Box: Technology and Economics.* Cambridge: Cambridge University Press.

Schumpeter, J. (1961) *Theory of Economic Development.* New York: Oxford University Press (1st edn 1911).

Smith, M. R. (ed.) (1985) *Military Enterprise and Technological Change.* Cambridge, Mass.: MIT Press.

Stamegna, M., Bonaiuti, C., Maranzano, P., Pianta, M. (2024) The economic impact of arms spending in Germany, Italy, and Spain, Peace Economics, Peace Science and Public Policy, https://doi.org/10.1515/peps-2024-0019

Strange, S. (ed.) (1984) *Paths to International Political Economy.* London: Allen & Unwin.

Thee, M. (1986) *Military Technology, Military Strategy and the Arms Race.* London: Croom Helm.

Thompson, E. P. (ed.) (1985) *Star Wars.* Harmondsworth: Penguin.

Tirman, I. (ed.) (1984) *The Militarization of High Technology.* Cambridge, Mass: Ballinger.

Ulbricht, L., & Egbert, S. (2024). In Palantir we trust? Regulation of data analysis platforms in public security. Big Data & Society, 11(3), 20539517241255108.

Van Der Vlist, F., Helmond, A., & Ferrari, F. (2024). Big AI: Cloud infrastructure dependence and the industrialisation of artificial intelligence. Big Data & Society, 11(1), 20539517241232630.

Zelikow, Ph., Cuéllar, M.-F., Schmidt, E., Matheny, J. (2024), Defense Against the AI Dark Arts: Threat Assessment and Coalition Defense, Hoover Institute essay, December 2024, Available at: https://www.hoover.org/research/defense-against-ai-dark-arts-threat-assessment-and-coalition-defense

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