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

Blurring boundaries: an analysis of the digital platforms-military nexus

Andrea Coveri [1]
Claudio Cozza [2]
Dario Guarascio [3]

[1] University of Urbino, Italy
[2] University of Naples Parthenope,Italy
[3] Sapienza University of Rome, Italy

2023/47 **December 2023**
ISSN(ONLINE) 2284-0400

Blurring boundaries: an analysis of the digital platforms-military nexus

Andrea Coveri*[1], Claudio Cozza†[2], Dario Guarascio‡[3]

[1] *University of Urbino Carlo Bo*
[2] *University of Naples Parthenope*
[3] *Sapienza University of Rome, GLO*

Abstract

This work analyzes the mutual dependence linking digital platforms, i.e., 'Big Tech', and the military apparatus. Three main elements are at the roots of such dependence: an 'originary linkage' binding the development of digital platforms with governments' R&D military efforts, the critical nature of infrastructures and technologies controlled by platforms, and their role as their government's 'eyes and ears' (both at home and abroad). Focusing on the US, we first document the growing relevance of these corporations as Department of Defence contractors. Second, we explore a selection of multi-year contracts entrusting platforms to develop and manage critical technologies and infrastructures for military purposes. Finally, we document the direct involvement of major US-based platforms in war scenarios.

JEL classification: L12, L22, P12.

Keywords: Monopoly capital, imperialism, war, nation-states, digital platforms, military industry.

"Everywhere do I perceive a certain conspiracy of rich men seeking their own advantage under the name and pretext of the commonwealth" (Sir Thomas More, 1516, as cited in Hobson, 1902).

"People of the same trade seldom meet together, even for merriment and diversion, but the conversation ends in a conspiracy against the public, or in some contrivance to raise prices" (Adam Smith, 1776).

*Corresponding author. Department of Economics, Society, Politics, University of Urbino Carlo Bo. E-mail address: andrea.coveri@uniurb.it

†Department of Economic and Legal Studies, University of Naples Parthenope. E-mail address: claudio.cozza@uniparthenope.it

‡Department of Law and Economics, Sapienza University of Rome. E-mail address: dario.guarascio@uniroma1.it

1 Introduction

Large digital platforms, also known as 'Big Tech', are now at the centre of attention in several streams of research, including economics, management studies, sociology, international political economy, labour law, and industrial relations. A number of reasons may explain their prominence. First of all, digital platforms have given rise to an unprecedented concentration of techno-economic power (Coveri et al., 2022; Vasudevan, 2022). Considering the major US-based platforms (e.g., Alphabet, Amazon and Apple), their overall market capitalisation is larger than the GDP of countries like Japan. The same goes if one looks at their Chinese counterparts, like Alibaba or Tencent (Jia et al., 2018; Li and Qi, 2022). This is largely associated with the staggering technological power that platforms concentrate in their hands, which is apparent when examining the distribution of patents on a global level in key fields such as Artificial Intelligence (AI): few platforms hold the majority share and the trend is in the direction of an even stronger concentration (Fanti et al., 2022; Calvino et al., 2023). It is therefore no coincidence that platforms are key stakeholders in the growing geopolitical tensions that pit the US and China against each other. Digital corporations directly (and often exclusively) control strategic knowledge, infrastructures and (dual) technologies of key relevance for both economic and military purposes (Farrell and Newman, 2019). In turn, geopolitical tensions ultimately affect the extent of platforms' global reach, the market outlets they have access to and the amount of data they can collect (Rikap and Flacher, 2020). Innovation patterns and ecosystems are also reshaped by the emergence of platforms (Lundvall and Rikap, 2022). On the one hand, the latter enables the mobilization (and combination) of knowledge and technologies with unprecedented speed and efficiency (Gawer, 2022; Jacobides et al., 2024). On the other hand, most of the relevant innovations are then siphoned out by large platforms – through, e.g., strategic acquisitions of start-ups – which are *de facto* shielded, if not strengthened, by innovation-based competition (Kurz, 2023). Moreover, the rise of platforms has challenged the very conceptualization of the firm (Pitelis, 2022). In fact, by monopolizing data (Zuboff, 2023), platforms exercise power and control far beyond their physical and legal perimeter, subordinating seemingly autonomous and distant organizations (Ietto-Gillies and Trentini, 2023). Finally, labour fragmentation is significantly exacerbated by platforms – both locally and on a global scale (Casilli et al., 2023) –, with relevant implications in terms of working conditions, economic vulnerability (see *inter alia*, Kenney and Zysman, 2020; Cirillo et al., 2023) and social conflicts (Della Porta et al., 2022).

What is relatively less investigated is the nexus linking large digital platforms and nation-states. Yet, this is a crucial dimension to be analyzed in order to understand why platforms have become so powerful and why such power is so difficult to undermine. Indeed, the fact that the state-corporation nexus is crucial to understanding the nature, behaviour, and systemic consequences of the firm was very clear to the Classical economists (e.g., Smith, 1776 and Marx, 1867). The converging strategies of monopolies (and cartels), on the one hand, and of colonial states, on the other, are at the heart of the theories of imperialism (Hobson, 1902; Lenin, 1917; Hilferding, 1923a). Likewise, the key role of the state in supporting large corporations, encouraging their internationalization, and bailing them out during downswings, is central to the Monopoly Capital (MC) tradition (Baran and Sweezy, 1966). In both cases, there is a peculiar component of the nation-state apparatus that plays a pivotal role: the military sector.

At the time of Hobson (1902)'s writings, military campaigns were crucial to open up new opportunities for capitalistic accumulation, secure productive inputs, and put competitors out of business. As capitalism expands across the globe and large transnational corporations (TNCs) come to increasingly shape its evolution, governments' military-related investments become essential to support capital accumulation, especially during stagnation phases (Baran and Sweezy, 1966). No less relevant, military-related R&D and public procurement assume a key role as vectors of technology transfer, especially for the development and introduction of radical innovations (Mowery, 2009). In the US case, the linkage between military-oriented R&D investments and the rise of high-tech TNCs

was at the basis of what, after WWII, has been popularized as the 'military-industrial complex' (Mowery, 2010). Since then, the latter has been one of the main ingredients of US military and technological hegemony (Galbraith, 2007). In this work, we explore the *mutual dependency* linking large digital corporations and the military sector, bridging imperialism studies (Lenin, 1917), the MC tradition (Baran and Sweezy, 1966) and more recent literature analysing the peculiar characteristics of platforms and the origins of their power (Conyon et al., 2022). We focus on the US, being the country where the first and most important digital platforms were developed (O'Mara, 2020), documenting both elements of continuity and discontinuity in the evolution of the US military-industrial complex (Pianta, 1989). In so doing, several research questions are addressed. First, to what extent the military sector is and has been relevant to the expansionary strategies of digital platforms? And, in turn, to what extent are platforms important for the military apparatus to pursue its objectives? Second, what is the role of platforms' techno-organizational characteristics in shaping their relationship with the military and intelligence activities? Third, what are the main differences between digital platforms and traditional defence contractors that usually partner with the US military sector (e.g., enterprises that stably supply armaments and equipment to the military)?

The analysis is developed along two main lines. First, building on previous studies (among others, Pianta, 1989; Mowery, 2009, 2010), we detect three main channels defining the platforms-military nexus: (i) the "originary linkage" and the role of technology transfer; (ii) the platforms' control of critical technologies and infrastructures and their role in the military-related supply chains; (iii) the peculiar position of platforms as 'eyes and ears' of the military apparatus. Second, we provide quantitative and qualitative evidence assessing: (i) the growing relevance of platforms as contractors of the US Department of Defence (DoD); (ii) the size and technological content of key DoD procurement contracts; (iii) the revolving doors linking platforms' boards and the military and security apparatuses; (iv) the active role platforms in warfare scenarios, with particular reference to the Russia-Ukraine conflict.

The paper is organized as follows. Section 2 reviews the literature on the state-corporation nexus, from the early stages of imperialism to the most recent developments in MC theory. Section 3 illustrates the main channels shaping the mutual dependence holding platforms and the military apparatus together. The quali-quantitative analysis is provided in Section 4 while Section 5 concludes, taking stock of the main results, discussing their implications and avenues for further research.

2 The State-corporation nexus: yesterday and today

According to liberal philosophy and neoclassical economics, the public and the private spheres are sharply separated. For classical liberalism, the public sphere is the (well-circumscribed) domain where the State pursues the collective interest, taking care of the public good (Hayek, 1946). In neoclassical economics, the State is there to provide those goods for which private incentives are missing, but that are essential for market interactions to take place (as in the tradition of both Old and New Welfare Economics) (see, e.g., Stiglitz, 1991). In this context, security and defence are, above all others, the activities through which the State preserves the community's superior values, beyond any particular private interest. By safeguarding social order internally and protecting the community against external threats, it allows free economic interactions to take place and, therefore, the maximization of social welfare to occur.

Classical economists used to have an antipodal (and yet more realistic) understanding of the State and its relationships with the private sphere. According to Adam Smith, one of the most common activities carried out by capitalists during the early stages of industrialization was to join their forces to 'conspire', aiming to influence the State to their own advantage (e.g., preventing regulations that may get in the way of their accumulation strategies). An even more radical rejection of the aforementioned separation can be found in Marx and Engels' Communist Manifesto: *'The executive of the modern state is [nothing] but a committee for managing the common affairs of the whole bourgeoisie'* (Marx and Engels, 1848).

As monopolies and cartels become capitalism's major driving forces and global conflicts loom on the horizon, a 'new stage of development' is reached (Lenin, 1917).[1] At the dawn of WWI, imperialism theories unravelled the peculiar role of the State and, more importantly, of its military apparatuses. The latter operate as 'internal forces', providing crucial support to the process of capitalistic accumulation (Hobson, 1902; Hilferding, 1923b).[2] Military campaigns are instrumental in entering new markets, seizing raw materials, expanding the pool of labour to be exploited, and cutting out competitors from the most advantageous trade routes. In turn, companies provide the State with capital goods and artefacts, including weapons, necessary to successfully conduct such campaigns. Not a harmonious division of roles aimed at ensuring peace and freedom, as suggested by liberal thinkers and neoclassical economists, but an 'alliance' in which the violence of the State and its hegemonic ambitions (Arrighi, 1981) are intertwined with the profit-maximization strategies of the monopolistic firm (Vasudevan, 2021).

The State-corporation nexus is also at the centre of the MC tradition (Baran and Sweezy, 1966), following along the lines traced by Lenin (1917).[3] In this literature, TNCs are the 'hubs' orchestrating the allocation of capital, domestically and internationally, giving rise to new forms of subordination and dependence (Hymer, 1960). These are also the *loci* where a large share of techno-organizational capabilities and innovations are developed, representing a key component of the emerging National Systems of Innovation (NSI) (Freeman, 1995). However, as global interconnectedness increases and sources of instability multiply, the state-TNC relationship becomes more complex. On the one hand, public demand results as a key source of reproduction and accumulation, particularly during downswings.[4] Similarly, science, R&D, and public procurement, a significant share of which stems from the military sector, represent a fundamental push for TNCs innovation and growth. On the other hand, growing complexity may turn into a misalignment of interests and conflicts.

As stressed by Hymer (1972) and discussed at length by Ietto-Gillies (2002), the rise of TNCs may resize the sovereign capacity of nation-states, diminishing their autonomy and weakening their ability to steer their own development trajectory. As a result, governments may respond by introducing regulations (e.g., tax, labour, antitrust and environmental laws) aimed at reducing TNCs room for manoeuvre. These are not the only sources of potential State-corporation conflicts, though. TNCs' internationalization strategies, including building ties with foreign governments to facilitate market penetration, may clash with their home state's foreign and defence policies (Ietto-Gillies, 2012). Again, reactions and countermeasures might be in order in an attempt to realign TNCs with their government goals. These conflicts are one of the key focus of Baran and Sweezy (1966)'s followers (among others, Cowling, 1982; Cowling and Sugden, 1998; Ietto-Gillies, 2012, 2021). In particular, the post-1970s MC literature concentrates its attention on the so-called 'retaliatory strategies' (Ietto-Gillies, 2012), put forth by TNCs to counter government actions that may limit their power and related value capture strategies. A typical example is the threat of moving production (and employment) from countries with strict to those with more permissive regulations concerning, for example, workers' rights or environmental protection (on this point, see Balcet and Ietto-Gillies, 2020). Therefore, marking a certain discontinuity with Lenin (1917)' view, the State is no longer seen (or not so explicitly) as an 'internal force' to corporations' strategies and, more broadly, to the process of accumulation. Rather, the emphasis is now on TNCs' attempts to affect those government actions (e.g., taxes and other redistributive measures, labor-protection laws, tariffs, investment subsidies, etc.) that can foster or

[1]Building on Hobson (1902) and Hilferding (1923b), Lenin (1917) proposed a new definition of 'Imperialism', conceived as *'capitalism at that stage of development at which the domination of monopolies and finance capital is established; in which the export of capital has acquired pronounced importance; in which the division of the world among the international trusts has begun; in which the division of all the territories of the globe among the biggest capitalist powers has been completed.'*

[2]During the same period, another popular definition of imperialism is provided by Rosa Luxemburg. According to her perspective, imperialism should be interpreted as the colonization, mostly aimed at exploiting human and natural resources, of "what remains still open of the non-capitalist environment" (Luxemburg, 2015).

[3]For a detailed review of MC theories see, among others, Foster (2014) and Sawyer (2022)

[4]According to Baran and Sweezy (1966), the growing dominance of TNCs is associated with the saturation of domestic markets and the exhaustion of profitable investment opportunities, leading to stagnation tendencies. Within this framework, states play a key role in providing monopolies with a way out of stagnation through defence spending.

hamper their growth (Cowling, 1982; Ietto-Gillies, 2012).[5]

The advent of digital platforms further reshapes the nature of the TNC, including its relationship with governments (Coveri et al., 2022). By way of illustration, Table A1 in the Appendix provides a synthetic account of the main discontinuities. While XX century's TNCs consolidate their presence at the times of managerial capitalism (Rahman and Thelen, 2019), digital platforms start rising when the neoliberal paradigm is fully established (Mudge, 2008). Platforms take hold when the large Taylorist (and then Toyotist) corporation is joined by smaller and more dynamic ICT companies, able to exploit network economies and operating in a context where state retrenchment, market liberalization, financial and trade globalization unfold at full steam. Moreover, platforms are able to rapidly expand their control (and associated value extraction) across countries, sectors and product segments by relying on a relatively smaller amount of foreign investments as compared to previous TNCs, i.e., the so-called 'FDI lightness' (Ietto-Gillies, 2021), and exploiting the close-to-zero marginal cost reproducibility of digital services (Coveri et al., 2022). This is lavishly rewarded by financial markets, with the capitalization of platforms growing relentlessly in spite of a relatively low dividends/revenues ratio (Kenney and Zysman, 2020; Li and Qi, 2022). Such a skyrocketing market capitalization further accelerates their growth, providing additional resources to invest, selectively, in R&D and M&A that are crucial to maintain control (and technological primacy) in relevant fields such as cloud computing and AI (Rikap et al., 2021; Fanti et al., 2022).

As the Internet becomes global, platforms magnify their ability to control data, digital technologies and related infrastructures (Rikap et al., 2021), as well as the new media where a large share of the public opinion is formed (Culpepper and Thelen, 2020). This has relevant consequences for the state-corporation nexus. First, platforms become indispensable partners in the production of public goods (e.g., the digitization of public services), both in the civilian and military spheres. This contributes to blurring the public-private boundaries, providing platforms with an 'infrastructural status' that can make them indistinguishable from the public operator. Second, the retaliatory power of platforms grows as compared to previous TNCs (Ietto-Gillies, 2021), as one of the peculiar domains under their control (e.g., social media) can determine whether political organizations are doomed to succeed or die.[6] Third, the control of *dual* technologies in security and defence-sensitive domains such as facial recognition, turn platforms into governments' 'eyes and hears', at home as well as abroad (see the next Section).

Such blurring boundaries and, most notably, the close connection with the security and military apparatuses make platforms key players in the confrontation between China and the US, the latter being largely played on the technological field (Rikap et al., 2021). Indeed, China is home to the largest non-US digital platforms having a global scale – e.g., Alibaba, ByteDance, Tencent – representing the most powerful challenger to the US technological (and, hence, military) supremacy (UNCTAD, 2019; Hötte et al., 2023). To give an example, the Chinese government has raised the Great Firewall to restrict access to US-based platforms, while promoting the development of its national champions (e.g., Alibaba and Tencent) to be part of its own (digital) military-industrial complex (Griffiths, 2021). Focusing on such confrontation, Rolf and Schindler (2023) argues that both the US and China 'leverage their domestic platforms to secure the control of data and extend their economic and military projection overseas'.

More than 100 years after Hobson (1902), digital platforms seem to vindicate some of the key arguments of the theory of imperialism, namely the convergence of economic strategies of TNCs and military (hegemonic) goals of nation states, the *crasis* between industrial and military apparatuses, and the blurring public-private boundaries. Of course, the shape of the state-corporation nexus is different and, as we will argue below, this is largely due to the peculiar and pervasive nature of the (dual) technologies that the platforms control.

[5] In this way, governments become, at least partially, 'external forces'. Therefore, the economic roots of imperialism – including the role of the military sector – are (at least analytically) lost. In the literature, these are replaced by explanations that super-ordinate the sociological or political dimensions of conflicts, as also Schumpeter (1972) does in *Imperialism and social classes*.

[6] A paradigmatic example is the Donald Trump's ban from Twitter and Facebook in 2021. See: https://www.nytimes.com/2022/05/10/technology/trump-social-media-ban-timeline.html

3 Mutual dependence and the digital platforms-military nexus

Several factors make governments dependent on TNCs. The latter generate a substantial share of output and employment, are a key 'complement' of foreign policy through FDIs and transnational alliances, and maintain assets and technological capabilities which result essential to govern change internally and exert hegemony externally (Arrighi, 1981). At the same time, TNCs are often reliant on their home governments' support to penetrate and expand in foreign markets (e.g., trade agreements, diplomatic activities aimed at facilitating the penetration in specific markets), resolve internal (e.g., legal and security activities to contrast workers, trade unions or local organization' struggles, on this point see also Balcet and Ietto-Gillies (2020)) and external (e.g., settling disputes with foreign governments or corporations) conflicts, mitigate demand constraints through public expenditure and investment (Baran and Sweezy, 1966), and support R&D projects characterized by radical uncertainty (Mazzucato, 2018).

Concerning digital platforms, what the latter need most is to escape regulations aimed at reducing their market power (e.g., antitrust policies, forced sale/separation of business units), restricting their capacity to extract and manipulate data (e.g., privacy policies as the EU's GDPR) or strengthening workers bargaining power (e.g., policies aimed at supporting unions). By the same token, platforms' systemic relevance further reinforces their position vis-à-vis governments, as the latter would hardly damage entities generating a substantial share of national income[7] and providing other firms with goods and services that are essential to carry out their economic activity.[8] More in general, the stronger the State-platforms mutual dependence, the lower the risk for the latter to face regulations that damage their economic and technological dominance (Vasudevan, 2022).

The military sector is where the state-corporation boundaries may become more blurred (Pianta, 1989; Foster and McChesney, 2014; Roland, 2021). In the context of the US military-industrial complex, a large literature has documented synergies as well as conflicts shaping the relationship between major contractors and the defence apparatus (see, among others, Markusen and Serfati, 2000; Dunne and Sköns, 2014; Smith, 2016).[9] While reviewing this vast literature goes beyond the scope of our contribution, three factors lying at the basis of the corporations-military nexus are worth stressing for our purposes. These elements have characterized the relationship between the state and corporations well before the advent of digital platforms. As the latter steps in, though, the same elements become key drivers of mutual dependence.

Originary linkage

An 'originary linkage' binds digital platforms and the military sector. During the 20th and, even more so, in the 21st century, most of the breakthroughs giving rise to new industries and technological paradigms were linked to military programs (Polanyi, 2015). These are based on long-term investments, path-breaking R&D activities and 'mission-oriented' projects in areas such as (i) infrastructures, from railroads to the Internet (O'Mara, 2020), (ii) aerospace (Mowery, 2009), (iii) raw materials and critical resources, aimed at ensuring the strategic autonomy of countries (Edler et al., 2023), and (iv) weapons and complementary goods needed for their development and deployment (Pianta, 1989). Major breakthroughs are often followed by 'technology transfer' to the benefit of newborn (or already existing) corporations that from there on will reap the advantages of their 'first-mover' status (Mazzucato, 2018). In turn, such a first-mover advantage may also increase the geo-strategic capacity of their home states.

[7] As of April 2023, the three major US-based digital corporations – i.e., Alphabet, Amazon and Meta – represented close to $3 trillion in market value. Data retrieved from STATISTA, available at: https://www.statista.com/statistics/277483/market-value-of-the-largest-internet-companies-worldwide/. Last access 15 July 2023.

[8] Large platforms provide vital services for companies operating in virtually all sectors, giving rise to what Cutolo and Kenney (2021) refer to as 'technological dependence'.

[9] The expression "industrial-military complex" was first coined and popularized by President Dwight D. Eisenhower in a famous speech delivered in January 1961.

There is large evidence on how military-related investments and R&D contributed to the emergence of new industries (see, among others, Mowery, 2010; Jacobsen, 2015).[10] In this regard, the Internet and most of the digital innovations following its establishment represent a textbook example (for a thorough account, see, among others, O'Mara, 2020). Mission-oriented projects carried out by major US Federal Agencies (e.g., the DARPA (Mowery, 2010)) contributed to the development of General-Purpose Technologies, including semiconductors (Dosi, 1984) or the TCP/IP protocol (Greenstein, 2020), that have been crucial for the diffusion of personal computers and, later on, of the Internet itself (Mazzucato, 2018). In other words, military R&D is to a significant extent behind the competitive advantage of the US in the nascent digital economy. Since the early days of the mainframe industry, US-based TNCs have taken the lion's share of global ICT markets with some competition coming, since the 1980s, from a bunch of Asian high-tech companies (Japanese, above all others).[11] In this context, the close relationships between DARPA, private corporations, and top universities favoured technology transfer, and incremental innovations and forged the US National Innovation System (NIS), including the Silicon Valley (SV). With the 'commercialization of the Internet' (Greenstein, 2015), the US competitive advantage consolidates and the pivotal role of its NIS stands out. By the late 1990s, SV-based companies – i.e. nowadays' dominant platforms such as Amazon, Google, and Facebook together with companies such as Apple and Microsoft that, since the 1980s, were already playing a significant role in the computer industry (O'Mara, 2020) – managed to catch the 'first train' to the newborn Internet economy, gaining dominant positions in critical market segments such as search engines (e.g., Google, now Alphabet), social networks (e.g., Facebook, now Meta), digital marketplaces (e.g., Amazon) and cloud services (e.g., AWS and Microsoft Azure).

That is, US platforms dominating the Internet economy owe their emergence to military projects supporting the development of basic knowledge and technologies and, no less importantly, favouring technology transfer (Mowery, 2010). This originary linkage, however, never fades away completely, even when the industries that emerged as a result of military-related R&D become mostly oriented towards private demand and civil purposes. In fact, military apparatuses continue to have an active role, affecting the evolutionary trajectory of products and technologies (Mazzucato, 2018) *via*, for example, military patents (Schmid, 2018). By the same token, institutions and procedures working as an 'always-open backdoor' for military apparatuses to monitor and, if needed, affect corporations' strategies are systematically established. As industry size and complexity increase and competition-driven incremental innovations dominate the evolutionary trajectory, the military may become relatively less active and 'visible' (Pianta, 1989). Nonetheless, formal (e.g., laws and regulations) and informal (e.g., moral suasion) ties are always in order (Lundvall and Rikap, 2022). Most notably, the active role of military-related institutions can return to the forefront, as is currently occurring with AI or quantum technologies (Gonzales, 2023), when resources and strategic direction are needed to push forward the technological frontier, especially when it comes to dual technologies with relevant security implications. As technological and geo-strategic conditions require it, the original linkage is revitalized and, with it, the integration of state-corporation strategies.

Knowledge, technology and critical infrastructures

Contemporary wars are to a significant extent digital (Merrin and Hoskins, 2020). The most advanced weapons (e.g., drones, missiles, aircrafts) and defence systems (e.g., anti-aircraft systems) are based on technologies such as AI (Johnson, 2019) or new-generation satellites. Cyber-attacks and

[10]The need to strengthen nation states strategic capabilities has always been among the key motivations behind public efforts in areas such as mining and infrastructure, which are not directly related to the military but which, in turn, can have a broader impact on the economic and technological sovereignty of nations. This is testified by the direct involvement of military resources in the development of such projects.

[11]Technological trajectories and related economic developments, however, are never static processes. Since the early 2000s, China's industrial policy tirelessly aimed to narrow the technological gap with the US. This has enabled China to achieve remarkable results that challenge the leadership of the US in key technology areas such as AI (Rikap et al., 2021), while the ongoing 'chip war' testifies to how intense the competition in this area has become (Miller, 2022).

actions aimed at preventing them are becoming a matter of life or death during armed conflicts. Likewise, digital technologies are essential to pursue security and intelligence activities (Brayne, 2020), both at home and abroad. Therefore, being on the digital frontier and, hence, preventing enemies from getting close to it is a fundamental objective for governments and their military apparatuses (Rolf and Schindler, 2023). As largely documented, such frontier is dominated by few global (US and Chinese) platforms (see, among others, Kemmerling and Trampusch, 2022). The latter monopolize key assets (i.e., servers, cloud infrastructures, submarine cables) (Gjesvik, 2023), hold the majoritarian share of digital patents (Fanti et al., 2022; Maslej et al., 2023) and are the locus where most of the formal and tacit knowledge, essential to move forward along technological trajectories (Dosi, 1982), is developed (Rikap et al., 2021). In this context, the state-platform mutual dependence is explained by both physical, formal, and tacit elements. First, the quasi-monopolistic control of technologies and infrastructures vital to the pursuit of military objectives makes platforms indispensable partners of their governments. The class of devices that goes by the name 'Internet of Military Things', comprising hardware and software technologies that can be deployed in military scenarios, is increasingly crucial in both physical and virtual battlefields.[12] Military operations involving the creation of a new surveillance system, access to sensitive information, protection from (or the perpetration of) a cyber-attack, or the deployment of a satellite system in remote, high-risk areas can hardly be realised without the cooperation of platforms. For the military, platforms' idiosyncratic competencies are particularly valuable and hard to reproduce, given their tacit and cumulative nature (Ietto-Gillies and Trentini, 2023). By the same token, as a digital infrastructure (e.g., cloud servers) grows in terms of size and relevance (e.g., increasing the mass of information stored and processed), the efficiency of embedded technologies (e.g., machine learning (ML) algorithms) and the uniqueness ('black-boxishness') of corporation-specific competencies increase too. This may strengthen platforms' position vis-à-vis both potential competitors as well as governments (Coveri et al., 2022).

Another element strengthening the state-platform mutual dependency is the pivotal role that the latter play in both civil and military innovation ecosystems (Rikap et al., 2021; Gawer, 2022; Jacobides et al., 2024). By governing knowledge co-creation processes and exploiting the modular structure of digital ecosystems, platforms benefit from the decentralized nature of digital innovation while preserving their economic and technological power. Similar dynamics apply to military-related supply chains. To digitize processes and products (including weapons), traditional suppliers (e.g., in the US case, Lockheed Martin, Raytheon, and Halliburton) cannot operate without the technologies, components, and related services provided (often under monopoly conditions) by platforms (on this point, see Wong and Younossi, 2023, and the next Section).

A third driver of dependence concerns skills and training activities. In high-tech industries, competencies tend to be complex, idiosyncratic, technology- and organization-specific (Dosi et al., 1994). As a result, attracting and developing the best skills is vital to preserve innovative capacity. However, in frontier fields such as Big Data, AI, or Quantum Computing there is no match in the competition between key digital corporations, on the one hand, other firms, and the government, on the other. This is due to the career prospects the former can offer and incomparable economic levers (e.g., stellar salaries and stock options) they can rely on (Rikap, 2023). As a result, the government may face a substantial dependence on key digital platforms, particularly when it comes to the introduction of new technological solutions and related training activities, as the latter tend to monopolize the skills needed to pursue such activities. No less relevant, sector-specific managerial competencies and relational networks make the top management of platforms essential partners in the digital transformation process, including that of the military apparatus. Given the urgency of the challenge, nation states, starting with the US and China, have no choice but to involve platforms' top managers in developing the most

[12] See: https://aws.amazon.com/it/blogs/iot/increase-military-readiness-with-aws-iot-for-defense-and-national-security/

strategic projects. As documented by Lundvall and Rikap (2022), such a role is often formalized in public bodies of acknowledged importance, including those aimed at designing military-related frontier technologies (e.g., AI).

Digital platforms as 'eyes and ears' of governments

Since the early days of the *East India Company*, the intermingling of the economic interests of TNCs, on the one hand, with diplomatic, intelligence and military activities of nation-states, on the other, used to be commonplace (Hobson, 1902). The overseas presence of corporations provides a unique tool for seizing sensitive information and managing relationships with local government and elites. Military and intelligence apparatuses, in turn, are often key partners of domestic corporations looking for foreign expansion: protecting assets and personnel, ensuring the security of logistics, and providing support in case of conflicts with local authorities and organizations. This convergence of expansionary strategies may be another key driver of mutual dependence, even at the time of digital platforms.

Instabilities in the government-corporation relationship, conflicts and contradictions are always in order, though. Corporations' expansionary strategies may clash with their home government's contingent geopolitical orientations. This can occur when companies forge close relationships with the foreign local government, despite the tensions that might exist between the latter and the companies' home country. Foreign policy, in turn, can be subject to sudden shocks and shifts, the latter being ill-matched with the fixed costs and long-term investments required by TNCs to penetrate foreign markets. In this respect, worsening (or, even more so, the impairment) relationships with a particular foreign country can represent a serious dry loss for the most exposed corporations (Rolf and Schindler, 2023). As a result, TNCs may activate their resources, e.g., lobbying (Culpepper, 2010), retaliatory power (Ietto-Gillies, 2012) or trying to influence politics through media control (Culpepper and Thelen, 2020), to avert the disruption of their economic activities in specific regions.

With the advent of digital platforms, the degree of mutual dependence increases substantially. At home, platforms are a fundamental 'arm' of their government's security, intelligence and law enforcement activities. On the one side, they play a key role in collecting data and information, which is crucial to prevent (and conduce) hacking, misinformation as well as digital attacks and threats to national security. For example, Microsoft has repeatedly shared threat assessments and reports of cyberattacks with the US government,[13] while Facebook and Twitter have intervened to stop disinformation campaigns by taking down networks of hijacked computer devices used to perform cyberattacks.[14] This inevitably leads these private corporations to assume a prominent role in assuring the national security, providing them with a responsibility which goes far beyond their core business while strengthening their bargaining and blackmail power vis-à-vis governments.

Abroad, platforms become 'eyes and ears' of their home state intelligence and military apparatuses. Platform-controlled information networks, including social media, are now a resource that governments cannot do without, even in pursuing security/military tasks. For example, in late 2022 it was reported that Twitter provided direct approval and internal protection to a vast network of online US military social media accounts by whitelisting a government bunch of social profiles. This network has been used by the DoD to directly influence public opinion in countries involved in war conflicts such as Yemen, Syria, Iraq, Kuwait and beyond.[15] On the other hand, once platforms have access to sensitive information, it is difficult for foreign governments to know what use will be made of it and to what extent this information will be transmitted and leveraged by platforms' home governments for security purposes.

[13]See https://www.nytimes.com/2023/07/11/us/politics/china-hack-us-government-microsoft.html; see also https://www.microsoft.com/en-us/security/business/security-intelligence-report

[14]See https://www.npr.org/2022/09/27/1125217316/facebook-takes-down-russian-network-impersonating-european-news-outlets; https://www.intelligence.senate.gov/sites/default/files/documents/os-jdorsey-090518.pdf

[15]See https://theintercept.com/2022/12/20/twitter-dod-us-military-accounts/

The limits to such a techno-infrastructural dependence, if any, are geopolitical. To avoid subjugation to US corporations (and, thus, to the partially integrated US intelligence and military apparatuses), countries such as China, Russia, or Iran have banned the former from accessing their domestic market, while supporting the growth of national platforms (e.g., the Chinese Alibaba, Tencent or JD) within their own national innovation network (Li and Qi, 2022). This strategy allowed China to develop its own platform ecosystem which, as in the US, is substantially integrated with the state and its civil and military apparatuses (Lundvall and Rikap, 2022; Rolf and Schindler, 2023).

More broadly, by partnering with digital corporations that control critical technologies and infrastructures – e.g., cloud (Rikap and Lundvall, 2022), AI (Fanti et al., 2022), blockchain (Beaumier and Kalomeni, 2022), 5G technology standard (Wu, 2020) and undersea cables (Gjesvik, 2023) – nation states (i.e., China and the US) can strengthen their grip on economies belonging to their 'sphere of influence', gain advantage over enemies or enact what Kwet (2019, p. 4) called 'digital colonialism'. The latter is described as a novel form of 'structural domination' based on the alliance between key digital corporations and the US government. Such domination is exercised through *"the centralised ownership and control of the three core pillars of the digital ecosystem: software, hardware, and network connectivity, which vests the United States with immense political, economic, and social power. As such, GAFAM (Google/Alphabet, Amazon, Facebook, Apple, and Microsoft) and other corporate giants, as well as state intelligence agencies like the National Security Agency (NSA), are the new imperialists in the international community. Assimilation into the tech products, models, and ideologies of foreign powers – led by the United States – constitutes a twenty-first century form of colonisation."*

In other words, being the exclusive suppliers of services for both business growth as well as for the strengthening of key public services (such as education and health), digital corporations become the 'tool' for ensuring economic and geopolitical subordination, particularly where digital penetration occurs in a pervasive manner (as in developing countries lacking substantial infrastructures, technologies and competences). Similar dynamics to the one documented by Kwet (2019), who focuses on the South African case, can be observed in the economies that have entered China's sphere of influence (Rolf and Schindler, 2023), which are increasingly subject to the strategies of the Chinese government and the technological dominance of its home-grown digital platforms such as Alibaba and Tencent (Keane and Yu, 2019).

4 The digital platforms-military nexus: an empirical assessment

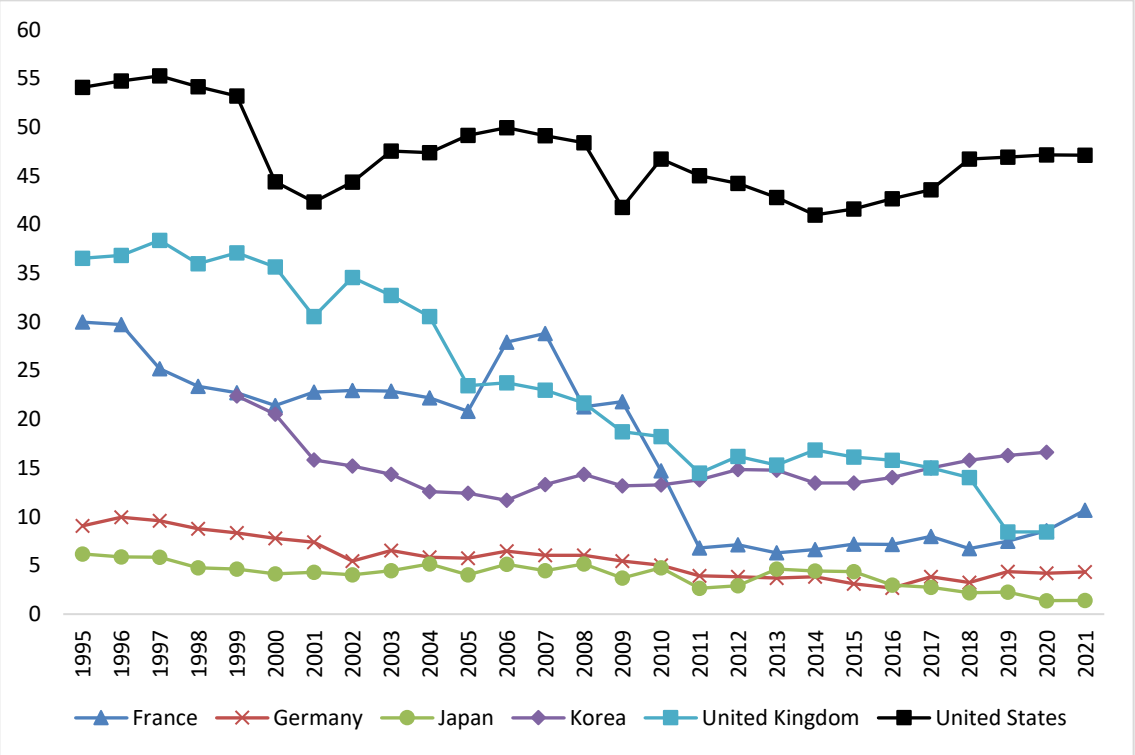
This section provides a quali-quantitative assessment of the digital platforms-military nexus in the US. In particular, we first analyze the evolution of the US Department of Defense (DoD) procurement contracts, showing the growing relevance of platforms as DoD contractors. Second, we delve into a set of major long-term contracts documenting the role of platforms as *dominus* of infrastructure and technologies (e.g., cloud, AI, satellites) that are not only critical to the achievement of military-related objectives (Shull et al., 2020), but also characterized by high complexity, cumulativeness and strong complementarity with their idiosyncratic capabilities (Mowery, 2010). Third, we document the 'revolving door' activity of former board members of US-based platforms moving to the military and security apparatuses (and vice versa), highlighting a further dimension of the integration between digital companies and government defence agencies. Finally, we analyze the available evidence on the active participation of key US-based platforms in the Russia-Ukraine war.

DoD procurement goes digital

To put the analysis in context, we begin by documenting the structural relevance of military-related R&D in the US. Figure 1 reports the government budget allocations for R&D (GBARD) for Defence from 1995 to 2021, focusing on the US and a set of selected Western economies. The figure shows that the share (%) of GBARD for defence over total GBARD for the US is much higher over the whole period than for all the other countries considered (France, Germany, Japan, South Korea and Japan), with the

former hovering around 55% in the second half of the 1990s and fluctuating around 45% in the first two decades of the 2000s (Mowery, 2009, 2010).

Figure 1. GBARD for Defence (% of total GBARD), selected countries, 1995-2021.

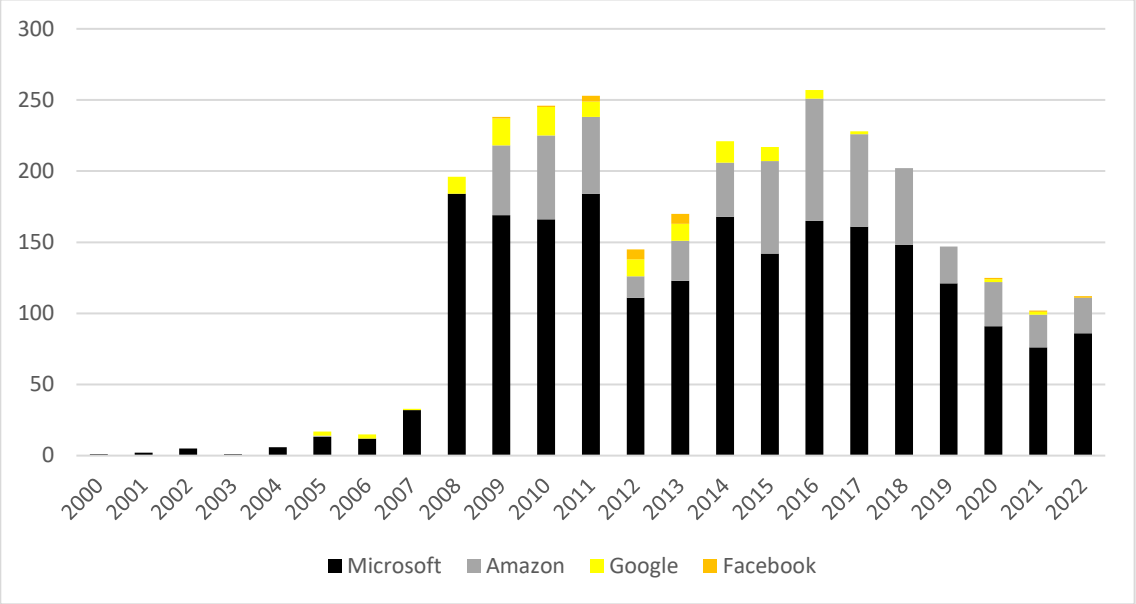


Source: authors' elaboration based on OECD data.

Further confirming this pattern, the US DoD's weapon systems acquisition funds requested for fiscal year (FY) 2024 are $315.0 billion – of which $170.0 billion is for Public Procurement and $145.0 billion for Research, Development, Test, and Evaluation –, up from $276.0 billion in the previous year. This increase is largely due to growing funding for cyberspace, spectrum, AI, 5G, and other emerging technologies in recent years, e.g., the DoD budget requests for the 'Command, Control, Communications, Computers, and Intelligence (C4I) Systems' mission almost doubled between 2017 and 2023, moving from $7.4 to $12.8 billion (DoD, 2023).

To shed light on the growing reliance of the US military apparatuses on technologies developed by digital platforms, we now dig into the official source of US public procurement data, i.e., *USAspending.gov*. Figure 2 shows the number of Alphabet (Google's parent company), Amazon, Facebook and Microsoft's contracts stipulated with US federal agencies (including the DoD) over the period 2000-2022. These figures highlight that a major acceleration in the total number of contracts awarded to digital corporations occurred since 2008. From then to 2018, digital platforms have been awarded more than 200 contracts per year, while a decreasing trend has been observed since 2019. The figure also shows that the lion's share of contracts was awarded to Microsoft and, to a lesser extent, Amazon. Finally, and consistently with the evidence provided by Maaser and Verlaan (2022), Alphabet and Facebook seem to be far less involved in military procurement.

Figure 2: Number of Amazon, Google, Facebook and Microsoft's contracts with all US federal agencies, 2000-2022.

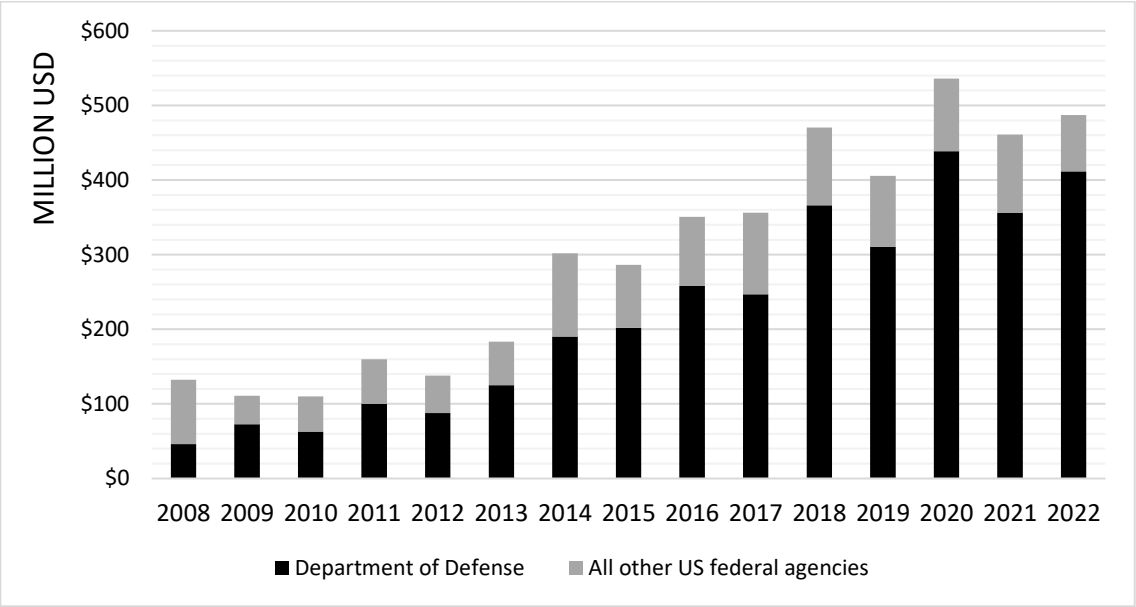


Source: authors' elaboration based on USAspending.gov data. Data updated to 18 January 2023.

Figure 3 reports the overall value of contracts awarded to digital platforms in monetary terms, distinguishing between those stipulated with the DoD and other US federal agencies. Overall, the figure shows that the monetary value of military (and security) procurement contracts has grown rather steadily from 2008 to 2021. Microsoft reports by far the greater value of both contracts with DoD and other US federal agencies: more than $4.4 billion over the whole period, of which about $3.2 billion was awarded by the DoD. This means that about 75% of the value of all US agencies' contracts stipulated with Microsoft were awarded by the DoD. Amazon follows at a distance: the value of contracts for this corporation is about $128 million over the whole period, of which about $50 million awarded by the DoD (equal to little less than 40% of the value of all contracts awarded to Amazon by US federal agencies).[16] Consistently with Figure 2, we find that the value of the contracts awarded to Alphabet and Facebook is relatively small (Maaser and Verlaan, 2022).

[16]If one includes the value of subcontracts, i.e., contracts awarded by US federal agencies to recipients that subcontracted part of the service to a platform, the situation does not change much. The value of the overall subcontracts awarded to Microsoft by all US federal agencies is equal to $1.7 billion over the whole period, of which about $1.4 billion (indirectly) was awarded by the DoD (82% of the overall value of subcontracts). As for Amazon, the value of the overall subcontracts awarded to this platform by all US federal agencies is equal to about 450 million over the whole period, of which slightly more than 200 million (indirectly awarded) by the DoD (45% of the overall value of subcontracts).

Figure 3: Total value of Amazon, Google, Facebook and Microsoft's contracts with the Department of Defense and other US federal agencies, 2008-2022.



Source: authors' elaboration based on USAspending.gov data. Data updated to 22 May 2023.

Critical technologies, infrastructures and services

The analysis of Federal procurement data lends support to the hypothesis of a growing reliance of the US military apparatuses on technologies controlled by large digital platforms. However, the share of US military procurement targeting such corporations appears to be negligible in absolute monetary terms, especially when compared to their revenues (e.g., Amazon reported total revenues of US$ 514 billion in 2022 and Microsoft US$ 198 billion in the same year). There are good reasons to believe that these data underestimate the role of platforms as relevant suppliers of the military apparatus (for a thorough investigation, see Maaser and Verlaan, 2022; Gonzales, 2023). In fact, *USAspending.gov* data do not include major contracts, mostly stipulated in recent years, according to which platforms are entrusted to develop (and often to directly manage) technologies and infrastructure related to security and military activities. This might be due to governments withholding disclosure of large contracts because of national security reasons; unclassified government contracts that are not included in the official US spending database; as well as the multi-year nature of such large awards, whose accounting allocation might make them less detectable (Paulson, 2021, 2022).

Building on several different sources (i.e., technical reports, companies' official documents and websites, and press articles), in what follows we thus document major publicly disclosed multi-year federal contracts entrusting platforms to develop and manage key technologies and infrastructures for military purposes (a systematic summary is provided by Table 1). According to these sources, the first deal between a leading digital platform and military apparatuses took place in early 2013, when the Central Intelligence Agency (CIA) awarded Amazon Web Services (AWS) with a contract worth up to $600 million over up to 10 years for providing computing cloud services to all 17 agencies that make up the intelligence community with the aim, *inter alia*, to prevent terrorist attacks.[17] Afterwards, in 2014, AWS launched its first "Top Secret Region", called "Top Secret-East", designed to host the US government's top-secret classified information. In 2017, this was followed by the launch of a second "Top Secret Region', called "Top Secret-West", providing additional cloud capacity for US intelligence and defence agencies, including the CIA and NSA.[18]

[17]See: https://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/. Last access: July 15 2023.

[18]See https://www.nextgov.com/emerging-tech/2021/12/amazon-web-services-announces-second-top-secret-cloud-region/187303/; see also: https://aws.amazon.com/it/blogs/publicsector/announcing-the-new-aws-secret-region/. Last access: Last access: July 15 2023.

Year and Department / Agency	Contractor	Value ($)	Nature of service	Declared aim
2013 – CIA	Amazon	600 million	Cloud	Data management aimed at preventing terrorist attacks
2019 – DoD	Alphabet (withdrawn); Amazon and Microsoft	50 million	Drones	Acquisition of AI technologies to improve image recognition in military drones – "Project Maven"
2020 – CIA	Alphabet, Amazon, Microsoft and Oracle	"Tens of billions"	Cloud	Cloud services centralized for 17 intelligence agencies – "Commercial Cloud Enterprise" (C2E) project
2021 – DoD	Microsoft	21.9 billion	Augmented reality visors	'HoloLens augmented reality headset' for military activities in highly complex contexts
2022 – NSA	Amazon	10 billion	Cloud	Cloud infrastructures for NSA ("Wild and Stormy" project)
2022 – DoD	Microsoft	NA	Stryker armoured vehicles	Digital devices to be incorporated into armed vehicles
2022 – DoD	Alphabet (Google public sector division)	NA	Google workspace	Provision of Google Workspace to 250,000 DoD employees
2022 – DoD	Alphabet, Amazon, Microsoft and Oracle	9 billion	Cloud	Cloud infrastructure for the "Joint Warfighting Cloud Capability" (JWCC)
2022 – DoD	Amazon and Microsoft	NA	Satellites	Space- and ground-based infrastructure for national security – "Hybrid Space Architecture" program

Table 1: Selection of multi-year military and security contracts signed by main US digital platforms

Such services are part of the AWS "Cloud Computing for U.S. Intelligence Community" project, which is aimed at providing federal agencies with technologies such as AI, ML and data analytics to save time and resources for warfighters and analysts. Notably, Microsoft launched similar cloud infrastructures for US national security missions, specifically aimed at speeding up the delivery of defence and security workloads classified as "top secret", i.e., the "Azure Government Top Secret" in 2021, following the announcement of "Azure Government Secret" in 2017.[19] Moreover, in November 2020, the CIA awarded AWS, Alphabet, IBM, Microsoft, and Oracle with its 'Commercial Cloud Enterprise' (C2E) contract to roll out new cloud hosting capabilities for the 17 federal intelligence agencies. These five digital corporations will compete for specific task orders over the next 15 years under a contract that could be worth "tens of billions" of dollars.[20] In April 2022, the NSA awarded a $10 billion cloud computing contract to AWS. This contract, called 'Wild and Stormy' (WaS), is a cloud computing services contract in support of the NSA's Hybrid Compute Initiative (HCI) aimed at addressing the NSA's significant and delicate processing and analytical requirements. Accordingly, AWS is the HCI cloud provider managing the process of moving the NSA's global intelligence and surveillance data from internal servers to the cloud.[21]

In June 2022, Alphabet announced the creation of 'Google Public Sector' (GPS), a new division aimed at helping US public sector entities accelerate their digital transformations. Few months later, GPS announced the provision of Google's workspace to 250.000 personnel of the U.S. Army. Then, in December 2022, Amazon, Google, Microsoft and Oracle were awarded a $ 9 billion contract under the Joint Warfighting Cloud Capability (JWCC), the latter first announced by the DoD in July 2021.[22] This project is designed to allow the Pentagon to fully leverage cloud capabilities developed by private corporations for military and defence-related activities, to foster "the nation's ability to stay a step ahead of adversaries."[23]

Under the JWCC contract, Google announced the "Google Cloud for the Department of Defense" and Amazon launched its "Cloud Computing for U.S. Defense", both aimed at providing warfighters with advanced technologies to be deployable in critical national security missions. For example, AWS was involved in a technical demonstration held in 2021 aimed at testing computing capabilities based on artificial intelligence (AI) and machine learning (ML) technologies for the Air Force's Advanced Battle Management System (ABMS), the latter being the Air Force's contribution to the Department of Defense's (DoD's) strategy to connect all branches of military forces in an "Internet of Military Things (IoMT)."[24] This follows the inclusion of AWS among the companies allowed to compete for "Indefinite Delivery/Indefinite Quantity" contracts, which give to these firms the opportunity to be awarded up with $950 million over five years for developing new digital capabilities for ABMS.[25] Another example regards the support provided by AWS to the development of "the first enduring tactical cloud presence" for the US Army's XVIII Airborne Corps, namely a US tactical force designed for rapid activities anywhere in the world.[26] Furthermore, AWS recently disclosed the availability for the US DoD customers of the AWS Modular Data Center – aimed at enabling the DoD to deploy self-contained data centers with built-in AWS infrastructure to store and analyze data in real-time "to gain military

[19]See: https://azure.microsoft.com/en-us/blog/announcing-new-azure-government-capabilities-for-classified-mission-critical-workloads/; see also https://azure.microsoft.com/en-us/blog/azure-government-top-secret-now-generally-available-for-us-national-security-missions/. Last access: July 15 2023.

[20]See: https://gcn.com/cloud-infrastructure/2020/11/cia-awards-massive-cloud-contract/315771/. Last access: July 15 2023.

[21]The WaS contract, once classified as secret, became public knowledge due to the legal dispute between Microsoft, which contended the attribution of the same, and the NSA. See https://www.crn.com/news/cloud/aws-wins-out-over-microsoft-for-10b-nsa-cloud-contract

[22]See: https://edition.cnn.com/2022/12/08/tech/pentagon-cloud-contract-big-tech/index.html

[23]For a description, see https://aws.amazon.com/blogs/publicsector/aws-selected-for-u-s-department-of-defense-joint-warfighting-cloud-capability-contract/.

[24]See: https://aws.amazon.com/it/blogs/publicsector/bringing-cloud-air-force-speed-of-mission-need/

[25]See: https://www.af.mil/News/Article-Display/Article/2359938/abms-signs-more-companies-post-onramp/

[26]See: https://aws.amazon.com/it/blogs/publicsector/aws-supports-development-u-s-armys-first-enduring-tactical-cloud-environment/

advantage in the most isolated environments"[27] – and of the AWS Snowblade, a device designed to compute, storage, and handle data for enabling defence warfighters to complete missions in highly risky locations.[28]

Besides providing cloud-based technologies and infrastructures for military purposes, platforms have also been major providers of cutting-hedge technology devices to be deployed in warfare scenarios. For example, in March 2021 Microsoft won a DoD contract for augmented reality headsets, worth up to $21.9 billion over 10 years. This includes 120,000 devices based on Microsoft's HoloLens augmented reality headset, enabling soldiers to fight, rehearse, and train in a single system. This contract follows a $480 million contract Microsoft received to give the Army prototypes of the Integrated Visual Augmented System (IVAS) in 2018.[29] Later that year, Amazon and Microsoft picked up $50 million contracts to develop AI surveillance software for US military drones after Google dropped Project Maven. The latter is a DoD programme launched in 2017 and designed to process full-motion images and video from drones to automatically detect potential targets. In 2018, more than 3,000 Google employees signed a petition expressing concern about the military use of AI, asking the company to abandon the project.[30] Following this protest, Google effectively abandoned the Maven project in early 2019,[31] being replaced by Microsoft, which started a $30 million contract in 2019, and AWS, which was awarded a $20 million in 2020.[32] However, both Google and its venture capital wing (i.e., Google Ventures) have maintained minority stakes in at least two companies supplying military surveillance tools, namely Orbital Insight and Planet. By the end of 2020, these companies had been awarded contracts worth more than $30 million with the DoD, alongside deals with the National Geospatial-Intelligence Agency (NGA), to which the Project Maven project was handed over by the DoD in 2022.[33] As for Microsoft, in August 2022 the US Army integrated the breakthrough technology that it designed into Stryker armoured vehicles in order to provide warfighters with enhanced capabilities to regain and maintain the upper hand in multi-domain battlefield operations.

Finally, it is worth reporting that, in May 2022, Amazon launched its first "AWS Defence Accelerator for startups", in partnership with a UK government technology firm. The main goal of the programme was to select start-up participants to foster their military and defence-related technological capabilities, such as cyber-defence solutions, data discovery and optimisation, and space exploitation, using cloud technologies. In early 2023, AWS broadened this project by launching the "AWS European Defence Accelerator", in partnership with another UK Government-supported innovation technology firm. Similar to the previous one, this project is aimed to train and support selected startups with AWS cloud technologies for developing defence-related technologies and capabilities for national security organizations across Europe.[34]

The provided evidence displays the growing importance of digital platforms as security and defence technology providers for federal agencies, especially the DoD (Maaser and Verlaan, 2022; Gonzales, 2023). This is in line with the more general Pentagon's long-term commitment to accelerate the adoption of commercially developed AI and cloud technologies for military use. In 1999, the CIA founded In-Q-Tel, a venture capital entity aimed at transferring the private sector's critical innovations into US intelligence and military apparatuses. More recently, in 2015, the DoD set up the Defense Innovation Unit Experimental (DIUx), later renamed Defense Innovation Unit (DIU), to promote a far stronger integration of US defence agencies with Silicon Valley's technological corporations by recruiting top talent and speed up the military procurement. The goal was to create a

[27]See https://aws.amazon.com/it/blogs/publicsector/announcing-aws-modular-data-center-u-s-department-defense-joint-warfighting-cloud-capability/

[28]See https://aws.amazon.com/about-aws/whats-new/2023/06/aws-snowblade-us-defense-jwcc-customers/

[29]See https://www.cnbc.com/2021/03/31/microsoft-wins-contract-to-make-modified-hololens-for-us-army.html.

[30]See https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html)

[31]See https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html)

[32]See https://www.forbes.com/sites/thomasbrewster/2021/09/08/project-maven-amazon-and-microsoft-get-50-million-in-pentagon-drone-surveillance-contracts-after-google/

[33]"Google Promised Not To Use Its AI In Weapons, So Why Is It Investing In Startups Straight Out Of 'Star Wars'?", Forbes, https://www.forbes.com/sites/thomasbrewster/2020/12/22/google-promised-not-to-use-its-ai-in-weapons-so-why-is-alphabet-investing-in-ai-satellite-startups-with-military-contracts/. Last access: 8 September 2023

[34]See https://aws.amazon.com/it/blogs/publicsector/aws-launches-2023-european-defence-accelerator-for-startups/

sort of "start-up accelerator" in cutting-edge technologies like AI, robotic systems, and cybersecurity, to build a more direct bridge linking the DoD and private corporations developing innovations with military applications.[35] Notably, the DIU also leads the US military's Hybrid Space Architecture (HSA), which in November 2022 awarded Microsoft Azure Space, AWS and Amazon's Project Kuiper – together with other defence tech start-ups – with contracts to improve space and ground-based communication infrastructures for national security.[36]

Revolving doors

Another sign of the platforms-military mutual dependence concerns the old-fashioned "revolving doors" mechanism. This pattern involves former top managers and executives of platforms becoming members of various government bodies linked to defence agencies and regulating commissions (and vice versa). On the one side, this is likely due to the imperative for governments to leverage the knowledge and networks maintained by former high-level platform executives to advance cutting-edge technologies for military-related initiatives (Lundvall and Rikap, 2022). One example is given by former vice-president of Apple, Doug Beck, recently appointed as the new director of the DIU.[37] Even more emblematic is the case of Eric Schmidt, former CEO of Alphabet. Together with former Secretary of State Henry Kissinger and ex-Deputy of Defense Secretary Robert Work,[38] Schmidt was a member of two government advisory boards – i.e., the Defense Innovation Advisory (DIA) Board and the National Security Commission on AI (NSCAI) – aimed at jump-starting technological innovation at the DoD to counter the emerging technological power of China. Nonetheless, Schmidt relied on his own venture capital to invest in defence start-ups, thus becoming a relevant actor on 'both sides of the table' at the same time.[39]

On the other side, the experience and contacts retrieved from working in governmental security apparatuses and the in-depth knowledge of evolving legislation make former members of government agencies key assets for digital corporations introducing technologies for which a regulatory framework has not yet been introduced; as well as for detecting strategies to elude or hamper legal procedures that may limit the applicability of their own technologies. Not surprisingly, several cases of former members of defence agencies transitioning into digital platforms' boards can be documented. For example, the former executive director of the Defense Innovation Advisory (DIA) Board, Josh Marcuse, in 2020 assumed the role of head of strategy and innovation for Google Public Sector, namely the department of Google developing technologies for public agencies, including the military apparatus. It is worth noting that, as executive director of the DIA since 2016, Marcuse was responsible for providing suggestions to the DoD, stood as an early supporter of the Joint Enterprise Defense Infrastructure (JEDI) cloud

[35]See: Kaplan, F., "The Pentagon's Innovation Experiment", *MIT Technology Review*, 19 December 2016, available at: https://www.technologyreview.com/2016/12/19/155246/the-pentagons-innovation-experiment/. Last access: 8 September 2023.

[36]See: Boyle, A., "Microsoft and Amazon take on new roles in Pentagon's space communication plans", *GeekWire*, 2 November 2022, available at: https://www.geekwire.com/2022/microsoft-amazon-pentagon-space-communication/. Last access: 8 September 2023.

[37]See: "DOD Announces Apple's Doug Beck as New Defense Innovation Unit Director", *Defense Innovation Unit* official website, 4 April 2023, available at: https://www.diu.mil/latest/dod-announces-apples-doug-beck-as-new-diu-director. Last access: 29 November 2023.

[38]As Deputy Secretary of Defense, in office from 2014 to mid-2017, Robert Work was also the major proponent and advocate of the so-called 'Third Offset', namely the competitive strategy aimed to leverage U.S. advanced technologies to offset China's and Russia's technological advances (Gentile et al., 2021).

[39]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: https://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.

procurement, and played a key role in formulating the ethical principles for the Joint Artificial Intelligence Center.[40]

Another example concerns retired US General Keith Alexander, former director of the National Security Agency (NSA) from August 2005 to March 2014 and commander of the U.S. Cyber Command from May 2010 to March 2014. In September 2020, it was disclosed that Alexander had assumed a position on Amazon's Board of Directors. Alexander's arrival was significant for Amazon, as it came amid the dispute with Microsoft over the $10 billion worth JEDI (Joint Enterprise Defense Infrastructure) contract with the DoD (later repealed and replaced in late 2021 by the JWCC documented above). Notably, Alexander's tenure at the NSA gained widespread attention due to the disclosure of classified documents by whistleblower Edward Snowden, unveiling extensive surveillance on both domestic and international communications conducted under Alexander oversight.[41]

A final case worth documenting concerns the revolving door between defence-related government agencies and Google divisions, in particular Google Public Sector. The board was established in June 2022 and includes, among others, retired generals from the US Air Force and Army, a former governor, and a CIA engineer who previously headed the CIA's Science and Technology Directorate.[42] This may not come as a surprise, since Google has hired dozens of CIA professionals in recent years. According to the Tech Transparency Project, from 2006 to 2016 there were 258 cases of "revolving door" activity between Google (or subsidiaries) and US federal agencies, including the CIA and other security agencies.[43]

Digital platforms go to war

Further evidence is provided focusing on the active participation of platforms into warfare activities. A case in point is the dreadful war in Ukraine, where major US-based platforms have assumed, since its very early stages, a direct role concerning the deployment of critical information-related infrastructures and technologies (Coveri et al., 2023). The archetype is SpaceX, the corporation providing a private satellite system used by the Ukrainian army (as well as by foreign military and intelligence personnel operating in the area) to carry out its operations.[44] Notably, in September 2022 the sudden shutdown of Starlink jeopardized a decisive military operation targeting Russian warships near the coast of Crimea. Musk recently stated that the shutdown was his deliberate decision, due to the fear that Russia might respond with nuclear weapons to the Ukraine attack. Shortly after these events, Elon Musk, the owner of SpaceX, finalized the acquisition of another key digital corporation — i.e., Twitter — and entered into negotiations with the US government (as well as its European allies) regarding the financing of Starlink.[45] A month later, Musk was reported (although he denied it) to hold a direct channel with Putin discussing his own 'peace plan' for Ukraine.[46]

Two elements stand out here. First, the crucial role played by a private corporation, whose activity is theoretically intended for the civil sphere, into a war, providing SpaceX with a stronger bargaining

[40]See Barnett, J., "Defense Innovation Board's Josh Marcuse heads to Google", *Fedscoop*, available at https://fedscoop.com/defense-innovation-board-google-josh-marcuse/. Last access: 29 November 2023.

[41]See Perez, M., "General Who Oversaw NSA Surveillance Collection Joins Amazon's Board Of Directors", *Forbes*, 9 September 2020, available at: https://www.forbes.com/sites/mattperez/2020/09/09/general-who-oversaw-nsa-surveillance-collection-joins-amazons-board-of-directors/. Last access 29 November 2023.

[42]See "Google Public Sector Appoints Its First Board of Directors", *govtech.com*, 17 May 2023, available at: https://www.govtech.com/biz/google-public-sector-appoints-its-first-board-of-directors. Last access: 29 November 2023.

[43]See "Google's US Revolving Door", *Tech Transparency Project*, 26 April 2016, available at: https://www.techtransparencyproject.org/articles/googles-revolving-door-us. Last access: 29 November 2023.

[44]See Srivastava, M., Olearchyk, R., Schwartz, F., & Miller, C. "Ukrainian forces report Starlink outages during push against Russia", *Financial Times,* 8 October 2022. Last access: 21 December 2023.

[45]On 1 June 2023, it was disclosed that Elon Musk's SpaceX was awarded a contract by Pentagon for the provision of the Starlink satellite system to be deployed in Ukraine. See "Elon Musk ordered Starlink to be turned off during Ukraine offensive, book says", *The Guardian*, 23 September 2023, available at: https://www.theguardian.com/technology/2023/sep/07/elon-musk-ordered-starlink-turned-off-ukraine-offensive-biography; "Elon Musk's SpaceX wins Pentagon contract for satellite in Ukraine", *Financial Times*, 1 June 2023, available at: https://www.ft.com/content/8503ed5a-5ca2-4d34-8c69-66ae92fa80dd).

[46]See https://fortune.com/2022/10/11/elon-musk-ian-bremmer-putin-russia-ukraine/

position vis-à-vis the government. Second, the military apparatus' heavy reliance on SpaceX technologies to pursue key battlefield objectives. Among other things, the latter may help explain the US government's overall malleability towards Musk's strategies, including those – such as the acquisition of Twitter – that could intensify the mutual dependence.

SpaceX is not alone in playing an active role in the Ukraine war, tough. AWS disclosed that, as early as February 24 2022, the day of the invasion, "members of the AWS public sector team met with members of the Ukrainian government. The discussion focused on bringing AWS Snowball devices (...) into Ukraine to help secure, store, and transfer data to the cloud."[47] Ukraine's largest private bank, PrivatBank, which serves 40 per cent of the Ukrainian population, has moved all its operations to the AWS cloud and stated that once the war is over, there will be no reason to go back anyway.[48] Since 6 October 2022, Amazon has also removed referral fees for Ukrainian small and medium enterprises selling their products on its European marketplace. And the same goes for Microsoft, Apple, Alphabet, and Meta. The former has committed to provide $100 million worth technology "to ensure that government agencies, critical infrastructure and other sectors in Ukraine can continue to serve citizens through the Microsoft Cloud".[49] Apple took the field by blocking Apple Pay electronic payments and stopping sales of its products in Russia, while Alphabet banned access to advertising and distribution of Russian state media and increased security measures for user access in Ukraine. Alphabet also blocked Russian state media channels RT and Sputnik from the Youtube platform, while Facebook (Meta) opted for excluding from Facebook and Instagram content stemming from media that are close to the Kremlin.

Overall, platforms' active participation in warfare activities is another element that may help explain the mutual dependence. As platforms become essential partners in pursuing a large number of military activities, the DoD is induced to seek stable and effective alliances with them. In this respect, the bargaining power of platforms may grow as they increase the amount of critical information under their control and the exclusivity of the technology-specific capabilities they develop. On the other hand, being involved in close relationships with military apparatuses, which operate with logics that differ from that of standard market relationships, exposes to risks and may reduce platforms' strategic and operational flexibility (Pianta, 1989). No less relevant, the integration between platforms and the military agencies could be threatened by the conflict between top managers, aimed at meeting DoD's demand, and highly skilled personnel – e.g., engineers and software developers – which may consider the development of war-related technologies ethically unacceptable (Gonzales, 2023).

5 Conclusions

According to imperialism studies and Monopoly Capital tradition, military expenditure and warfare are the result of governments' active role in supporting the capital accumulation of monopolistic corporations. Although with important differences among them, authors belonging to these schools have highlighted the convergence of interests and strategies on the part of the state, on the one hand, and monopoly capital, on the other, as an intrinsic feature of capitalist accumulation and the driving force of inter-imperialist conflicts.

Building on these theories, in this work we attempted to show how digital platforms present both similarities and discontinuities in the state-corporations relationship, 'blurring' its boundaries and giving rise to a form of 'mutual dependence'. In particular, three main elements lying at the basis of the state-platforms mutual dependence were detected: an 'originary linkage' binding the development of giant privately-owned platforms with governments' R&D military efforts, the critical nature of infrastructures and technologies controlled by digital platforms, and their role as their government's

[47] https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future

[48] *Ibidem.*

[49] See: "Microsoft extends free tech support for Ukraine through 2023", *Reuters*, 3 November 2022, available at: https://www.reuters.com/technology/microsoft-extends-free-tech-support-ukraine-through-2023-2022-11-03/. Last access: 29 November 2023.

'eyes and ears' (both at home and abroad). In addition to their systemic relevance – allowing platforms to activate effective 'retaliatory power' vis-à-vis public authorities (Ietto-Gillies, 2012) –, the state-platforms dependence is fundamentally related to the complex, cumulative and idiosyncratic nature of the productive and technological capabilities developed and mastered by digital corporations. We contended that this is especially true in the security and military sector, where technological dependence is magnified, and the state-platforms overlap turns out to be substantial. On the other hand, we showed that the resources and support that the State provides to platforms are of utmost importance as an accumulation mean, demand-pull innovation driver as well as a tool to break down barriers to domestic and foreign expansion.

Leveraging quantitative and qualitative data and focusing on the US case, we also documented the growing prominence of platforms as DoD contractors, which goes hand in hand with their role as developers and masters of key strategic information-related infrastructures. Finally, digital platforms differ from more traditional TNCs insofar as they are not only critical suppliers to military agencies and traditional military suppliers. Remarkably enough, these corporations develop and deploy the same dual technologies that enable them to dominate the digital market to also play an active role in war scenarios, such as the current war in Ukraine.

The relationship between the state and corporations (including platforms) is much more complex than what has been conveyed here, making further research much needed. In this respect, three elements are worth mentioning. Although we emphasized the convergence between corporate and state strategies, the latter can easily clash to the extent that, for example, the expansion of the former leads to actions contradicting the objectives of the latter (and vice versa). Additionally, we have not taken into account the fragmented and conflictual nature of public authorities, including the political dimension. The State and its apparatuses are not monolithic, as interest groups in perpetual conflict shape their forms and orientation, including relationships with corporations. This can have significant effects on the degree of State-platforms mutual dependence. Likewise, a stronger reliance on platforms by government agencies can influence the forms and evolution of public institutions.

Finally, this work casts a sinister light on digital technologies, often naively considered as 'neutral' and capable of indiscriminately improving the human condition. On the contrary, if their development is bound between the support of monopolistic interests and the design of technologies suitable for effective surveillance and killing, social discontent could result in a brand new 'luddism'. At this time, not driven (or not solely) by the fear of mass unemployment, but by a more general desire to preserve the human race from the perverse alliance of public and private sorcerer's apprentices (assuming that this distinction makes any sense). We believe, however, that this risk can be averted, provided that one is willing to question the subordination of the production of knowledge and digital technologies to the expansionist strategies of platforms and states, in favour of their radical reorientation towards the satisfaction of social needs.

References

Arrighi, G. (1981). The geometry of imperialism: The limits of Hobson's paradigm. *Science and Society 45*(4).

Balcet, G. and G. Ietto-Gillies (2020). Internationalisation, outsourcing and labour fragmentation: the case of fiat. *Cambridge Journal of Economics 44*(1), 105–128.

Baran, P. A. and P. M. Sweezy (1966). *Monopoly Capital. An Essay on the American Economic and Social Order*. Monthly Review press Press.

Beaumier, G. and K. Kalomeni (2022). Ruling through technology: politicizing blockchain services. *Review of International Political Economy 29*(6), 2135–2158.

Brayne, S. (2020). *Predict and Surveil: Data, discretion, and the future of policing*. Oxford University Press, USA.

Calvino, F., C. Criscuolo, H. Dernis, and L. Samek (2023). What technologies are at the core of ai?: An exploration based on patent data.

Casilli, A., J. Torres-Cierpe, F. De Stavola, and G. Peterlongo (2023). From gafam to rum: Platforms and resourcefulness in the global south. *Pouvoirs 185*(2), 51–67.

Cirillo, V., D. Guarascio, and Z. Parolin (2023). Platform work and economic insecurity in italy. *Structural Change and Economic Dynamics 65*, 126–138.

Conyon, M., M. Ellman, C. N. Pitelis, A. Shipman, and P. R. Tomlinson (2022). Big tech oligopolies, keith cowling, and monopoly capitalism.

Coveri, A., C. Cozza, and D. Guarascio (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., C. Cozza, and D. Guarascio (2023). War in the time of digital platforms. *Social Europe, Available at: https://www.socialeurope.eu/war-in-the-time-of-digital-platforms*.

Cowling, K. (1982). *Monopoly capitalism*. Macmillan International Higher Education.

Cowling, K. and R. Sugden (1998). The essence of the modern corporation: markets, strategic decision-making and the theory of the firm. *The Manchester School 66*(1), 59–86.

Culpepper, P. D. (2010). *Quiet politics and business power: Corporate control in Europe and Japan*. Cambridge University Press.

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

Cutolo, D. and M. Kenney (2021). Platform-dependent entrepreneurs: Power asymmetries, risks, and strategies in the platform economy. *Academy of Management Perspectives 35*(4), 584–605.

Della Porta, D., R. E. Chesta, and L. Cini (2022). *Labour Conflicts in the Digital Age: A Comparative Perspective*. Policy Press.

DoD (2023). Fiscal year 2024 program acquisition costs by weapon system.

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. (1984). *Technical change and industrial transformation: the theory and an application to the semiconductor industry*. Springer.

Dosi, G., L. Marengo, et al. (1994). Some elements of an evolutionary theory of organizational competences. *Evolutionary concepts in contemporary economics*, 157–178.

Dunne, J. P. and E. Sköns (2014). The military industrial complex. In *The global arms trade*, pp. 281–292. Routledge.

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

Fanti, L., D. Guarascio, and M. Moggi (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. and A. L. Newman (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security 44*(1), 42–79.

Foster, J. B. (2014). *The theory of monopoly capitalism*. NYU Press.

Foster, J. B. and R. McChesney (2014). Surveillance capitalism. *Monthly review 66*(3), 1–31.

Freeman, C. (1995). The 'national system of innovation'in historical perspective. *Cambridge Journal of economics 19*(1), 5–24.

Galbraith, J. K. (2007). *The new industrial state*, Volume 9. Princeton University Press.

Gawer, A. (2022). Digital platforms and ecosystems: remarks on the dominant organizational forms of the digital age. *Innovation 24*(1), 110–124.

Gentile, G. P., M. R. Shurkin, A. T. Evans, M. Grisé, M. Hvizda, and R. Jensen (2021). *A History of the Third Offset, 2014-2018*. RAND Corporation Santa Monica, CA.

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

Gonzales, R. (2023). Militarising big tech. the rise of silicon valley's digital defence industry. *TNI, Available at: https://www.tni.org/en/article/militarising-big-tech*, 1–12.

Greenstein, S. (2015). *How the internet became commercial: Innovation, privatization, and the birth of a new network*. Princeton University Press.

Greenstein, S. (2020). The basic economics of internet infrastructure. *Journal of Economic Perspectives 34*(2), 192–214.

Griffiths, J. (2021). *The great firewall of China: How to build and control an alternative version of the internet*. Bloomsbury Publishing.

Hayek, F. A. (1946). *Individualism: true and false*. Hodges, Figgis & Company.

Hilferding, R. (1908 [1923]b). *Das finanzkapital*. Wien: Verlag der Wiener Volksbuchhandlung.

Hilferding, R. (1923a). *Das finanzkapital*, Volume 3. Verlag der Wiener Volksbuchhandlung.

Hobson, J. (1902). *Imperialism, A Study*. New York: James Pott and Company.

Hötte, K., T. Tarannum, V. Verendel, and L. Bennett (2023). Ai technological trajectories in patent data.

Hymer, S. (1972). The internationalization of capital. *Journal of economic issues 6*(1), 91–111.

Hymer, S. H. (1960). *The international operations of national firms, a study of direct foreign investment*. Ph. D. thesis, Massachusetts Institute of Technology.

Ietto-Gillies, G. (2002). *Transnational corporations: Fragmentation amidst integration*, Volume 29. Routledge. Ietto-Gillies, G. (2012). *Transnational corporations and international production: concepts, theories and effects*.
Edward Elgar Publishing.

Ietto-Gillies, G. (2021). Transnationality in the xxi century. concept and indicators. *critical perspectives on international business*.

Ietto-Gillies, G. and C. Trentini (2023). Sectoral structure and the digital era. conceptual and empirical analysis. *Structural Change and Economic Dynamics 64*(C), 13–24.

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

Jacobsen, A. (2015). *The Pentagon's Brain: An Uncensored History of DARPA, America's Top-secret Military Research Agency*. Hachette UK.

Jia, K., M. Kenney, and J. Zysman (2018). Global competitors? mapping the internationalization strategies of chinese digital platform firms. In *International business in the information and digital age*, pp. 187–215. Emerald Publishing Limited.

Johnson, J. (2019). Artificial intelligence & future warfare: implications for international security. *Defense & Security Analysis 35*(2), 147–169.

Keane, M. and H. Yu (2019). A digital empire in the making: China's outbound digital platforms. *International Journal of Communication 13*, 4624–4641.

Kemmerling, M. and C. Trampusch (2022). Digital power resources (dpr): The political economy of structural and infrastructural business power in digital (ized) capitalism. *Socio-Economic Review*, mwac059.

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.

Kurz, M. (2023). *The market power of technology: Understanding the second gilded age*. Columbia University Press.

Kwet, M. (2019). Digital colonialism: Us empire and the new imperialism in the global south. *Race & Class 60*(4), 3–26.

Lenin, V. (1963 [1917]). *Imperialism, the Highest Stage of Capitalism*. Moskow: Progress Publisher.

Li, Z. and H. Qi (2022). Platform power: monopolisation and financialisation in the era of big tech. *Cambridge Journal of Economics 46*(6), 1289–1314.

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.

Luxemburg, R. (2015). *The accumulation of capital*. Routledge.

Maaser, L. and S. Verlaan (2022). Big tech goes to war. *Studien 5*, 2022.

Markusen, A. and C. Serfati (2000). Remaking the military industrial relationship: A french-american comparison. *Defence and peace economics 11*(1), 271–299.

Marx, K. (2004 [1867]). *Capital: volume I*. Penguin UK.

Marx, K. and F. Engels (1967 [1848]). The communist manifesto. 1848. *Trans. Samuel Moore. London: Penguin 15*(10.1215), 9780822392583–049.

Maslej, N., L. Fattorini, E. Brynjolfsson, J. Etchemendy, K. Ligett, T. Lyons, J. Manyika, H. Ngo, J. C. Niebles, V. Parli, et al. (2023). The ai index 2023 annual report. *AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, Stanford, CA*.

Mazzucato, M. (2018). Mission-oriented innovation policies: challenges and opportunities. *Industrial and Corporate Change 27*(5), 803–815.

Merrin, W. and A. Hoskins (2020). Tweet fast and kill things: Digital war. *Digital War 1*, 184–193.

Miller, C. (2022). *Chip war: the fight for the world's most critical technology*. Simon and Schuster.

Mowery, D. C. (2009). National security and national innovation systems. *The Journal of Technology Transfer 34*(5), 455–473.

Mowery, D. C. (2010). Military r&d and innovation. In *Handbook of the Economics of Innovation*, Volume 2, pp. 1219–1256. Elsevier.

Mudge, S. L. (2008). What is neo-liberalism? *Socio-economic review 6*(4), 703–731.

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

Paulson, R. (2021). Tech inquiry report 2021. *Public Available Information - PAI, Available at: https://techinquiry.org/EasyAsPAI/resources/EasyAsPAI.pdf 5*, 1–42.

Paulson, R. (2022). Tech inquiry report 2022. *Public Available Information - PAI, Available at: https://techinquiry.org/docs/InternationalCloud.pdf* , 1–154.

Pianta, M. (1989). High technology programmes: for the military or for the economy? In *Making Peace Possible*, pp. 185–217. Elsevier.

Pitelis, C. (2022). Big tech and platform-enabled multinational corporate capital (ism): the socialisation of capital, and the private appropriation of social value. *Cambridge Journal of Economics*.

Polanyi, K. (2015). *The great transformation*.

Rahman, K. S. and K. Thelen (2019). The rise of the platform business model and the transformation of twenty-first-century capitalism. *Politics & society 47*(2), 177–204.

Rikap, C. (2023). *Same End by Different Means: Google, Amazon, Microsoft and Meta's Strategies to Organize Their Frontier AI Innovation Systems*. City, University of London.

Rikap, C. and D. Flacher (2020). Who collects intellectual rents from knowledge and innovation hubs? questioning the sustainability of the singapore model. *Structural Change and Economic Dynamics 55*, 59–73.

Rikap, C. and B.-Å. Lundvall (2022). Big tech, knowledge predation and the implications for development. *Innovation and Development 12*(3), 389–416.

Rikap, C., B.-Å. Lundvall, et al. (2021). The digital innovation race. *Springer Books*.

Roland, A. (2021). *Delta of Power: The Military-Industrial Complex*. JHU Press.

Rolf, S. and S. Schindler (2023). The us–china rivalry and the emergence of state platform capitalism. *Environment and Planning A: Economy and Space*, 0308518X221146545.

Sawyer, M. (2022). Monopoly capitalism in the past four decades. *Cambridge Journal of Economics*.

Schmid, J. (2018). The diffusion of military technology. *Defence and Peace Economics 29*(6), 595–613.

Schumpeter, J. A. (1972). *Imperialism and Social Classes: Two Essays*. Ludwig von Mises Institute.

Shull, A., D. Araya, S. Bradshaw, A. S. Gill, M. C. Horowitz, M. King, R. Mazzolin, M. Medeiros, R. Nieto-Gómez, and L. Vihul (2020). Modern conflict and artificial intelligence.

Smith, R. (2016). *Military economics: the interaction of power and money*. Springer.

Stiglitz, J. E. (1991). The invisible hand and modern welfare economics.

UNCTAD (2019). Digital economy report 2019. value creation and capture: Implications for developing countries.

Vasudevan, R. (2021). The network of empire and universal capitalism: imperialism and the laws of capitalist competition. *Review of Social Economy 79*(1), 76–102.

Vasudevan, R. (2022). Digital platforms: monopoly capital through a classical-marxian lens. *Cambridge Journal of Economics*.

Wong, J. and O. Younossi (2023). Improving defense acquisition: Insight from three decades of rand research. Technical report, Acquisition Research Program.

Wu, X. (2020). Technology, power, and uncontrolled great power strategic competition between China and the United States. *China International Strategy Review 2*(1), 99–119.

Zuboff, S. (2023). The age of surveillance capitalism. In *Social Theory Re-Wired*, pp. 203–213. Routledge.

6 Appendix

	XX Century TNC	Digital platforms
Capitalistic phase	Managerial	Neo-liberal
Dominant sector	Manufacturing	Services
Strategic objectives	Controlling the economic space by expanding physical assets and (to a lower extent) intangible ones (e.g., patents, trademarks)	Controlling (selectively) physical assets and (extensively) intangibles, data and data-related infrastructures
Growth drivers	Supply-side economies of scale	Supply and demand-side economies of scale (e.g., two-side network effects)
Capital structure	Concentration and centralization	Centralization without concentration
Corporate governance	High profits and dividend pay-out ratio	Relatively low profits/revenue ratio, share-holder buyback, selective investments to control data-related infrastructures
Internationalization strategies	Massive FDIs, directly exercised hierarchical control along the SC, centralization of R&D	FDI lightness, externalization and indirect control, dominance over the innovation ecosystem
Control over the labor force	Taylorism/Toyotism	Digital Taylorism
Control over demand flows	Marketing and advertising	Targted ads, 'anticipation' of demand flows, induced behavior
State-corporation nexus	Lobbying activities and retaliatory power	Lobbying, retaliatory power magnified by the control of data and related infrastructures

Table A1: XX Century TNCs vs digital platforms