Routledge
Taylor & Francis Group

Review of Political Economy

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/crpe20

# Blurring Boundaries: An Analysis of the Digital Platforms-Military Nexus

Andrea Coveri, Claudio Cozza & Dario Guarascio

**To cite this article:** Andrea Coveri, Claudio Cozza & Dario Guarascio (03 Sep 2024): Blurring Boundaries: An Analysis of the Digital Platforms-Military Nexus, Review of Political Economy, DOI: 10.1080/09538259.2024.2395832

**To link to this article:** https://doi.org/10.1080/09538259.2024.2395832

Published online: 03 Sep 2024.

REVIEW OF POLITICAL ECONOMY
https://doi.org/10.1080/09538259.2024.2395832



# Blurring Boundaries: An Analysis of the Digital Platforms-Military Nexus

Andrea Coveri [a], Claudio Cozza [b] and Dario Guarascio [c]

[a]University of Urbino, Urbino, Italy; [b]University of Naples 'Parthenope', Napoli, Italy; [c]Sapienza University of Rome, Rome, Italy

**ABSTRACT**

This work analyses the mutual dependence linking digital platforms, i.e., 'Big Tech', and the US military apparatus. Three main elements at the roots of such dependence are detected: an 'originary linkage' binding the development of digital platforms with governments' military R&D 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 US Department of Defense 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.

**ARTICLE HISTORY**
Received 26 December 2023
Accepted 19 August 2024

**KEYWORDS**
Monopoly capital; imperialism; war; digital platforms; military industry

**JEL CODES**
L12; L22; P12

> 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)
>
> If necessity is the mother of invention, war is the midwife of innovation
>
> (Eric Schmidt, former Alphabet CEO)[1]

## 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 factors may explain their prominence. First of all, digital platforms have given rise to an

**CONTACT** Andrea Coveri andrea.coveri@uniurb.it
[1]See Schmidt (2023).

unprecedented concentration of techno-economic power (Coveri, Cozza, and Guarascio 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, Kenney, and Zysman 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, Guarascio, and Moggi 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 the 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, large digital corporations enable the mobilisation (and combination) of knowledge and technologies with unprecedented speed and efficiency (Gawer 2022; Jacobides, Cennamo, and Gawer 2024). On the other hand, most of the relevant innovations are then siphoned off 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 conceptualisation of the firm (Pitelis 2022). In fact, by monopolising data (Zuboff 2019), platforms exercise power and control far beyond their physical and legal perimeter, subordinating seemingly autonomous and distant organisations (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, Guarascio, and Parolin 2023) and social conflicts (Della Porta, Chesta, and Cini 2022).

What is relatively less investigated is the nexus linking large digital platforms and nation states. Yet, this is a crucial dimension to be analysed 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 and Marx (1867 [2004]). 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; Hilferding 1910; Lenin 1917 [1963]). Likewise, the key role of the state in supporting large corporations, encouraging their internationalisation, 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's writing (1902), military campaigns were crucial to create 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) increasingly shape its evolution, governments' military-related investments become essential for supporting 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 popularised 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 [1963]), the MC tradition (Baran and Sweezy 1966) and the more recent literature analysing the peculiar characteristics of platforms and the origins of their power (Conyon et al. 2022).

In doing so, we provide one of the first exploratory contributions to an under-investigated research domain. The analysis focuses 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). Three research questions are addressed. First, to what extent is and has the military sector 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? Third, what is the role of platforms' techno-organisational characteristics in shaping their relationship with the military and intelligence activities?

The analysis evolves 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 Defense (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 play in warfare scenarios, with particular reference to the Russo-Ukrainian War.

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

## 2. The State-Corporation Nexus: Yesterday and Today

According to neoclassical economics, the public and the private spheres are sharply separated. The public sphere, in particular, is conceived as the (well-circumscribed) domain where the state pursues the collective interest, taking care of the public good (Roncaglia

2005). The role of the state is thus essentially 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 maximisation of social welfare to occur.

Classical economists used to have an antipodal (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 industrialisation 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' *The 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 [1967]).

As monopolies and cartels became capitalism's major driving forces and global conflicts loomed on the horizon, a 'new stage of development' was reached (Lenin 1917 [1963]).[2] 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 1910).[3] 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 1978) are intertwined with the profit-maximisation strategies of the monopolistic firm (Vasudevan 2021).

The state-corporation nexus is also at the centre of the MC tradition (Baran and Sweezy 1966), along the lines traced by Lenin (1917 [1963]).[4] 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 [1976], 1970). These are also the loci where a large share of techno-organisational 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

[2]Building on Hobson (1902) and Hilferding (1910), Lenin (1917 [1963]) 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.'

[3]During the same period, another popular definition of imperialism is provided by Rosa Luxemburg. According to her perspective, imperialism should be interpreted as the colonisation, mostly aimed at exploiting human and natural resources, of 'what remains still open of the non-capitalist environment' (Luxemburg 1913 [2003]).

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

complex. On the one hand, public demand results in being a key source of reproduction and accumulation, particularly during downswings.[5] Similarly, science, R&D, and public procurement, a significant share of which stems from the military sector, are a fundamental driver of 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' internationalisation 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 issues that the followers of Baran and Sweezy (1966) (among others, Cowling 1982; Cowling and Sugden 1998; Ietto-Gillies 2012, 2021) focus on. In particular, post-1970s MC literature concentrates on the so-called 'retaliatory strategies' (Ietto-Gillies 2012) put forth by TNCs to counter government actions that may limit their power, as well as the 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 [1963])'s 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, labour-protection laws, tariffs, investment subsidies, etc.) that can foster/hamper their growth (Cowling 1982; Ietto-Gillies 2012).[6]

The advent of digital platforms further reshapes the nature of the TNC, including its relationship with governments (Coveri, Cozza, and Guarascio 2022). By way of illustration, Table A1 in the Appendix provides a synthetic account of the main discontinuities. While 20th century TNCs consolidate their presence at an era 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 liberalisation, and financial and trade globalisation 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'

[5]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 defense spending.

[6]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, they are replaced by explanations that super-ordinate the sociological or political dimensions of conflicts, as also Schumpeter (1951) does in Imperialism and social classes.

(Ietto-Gillies 2021), and by exploiting the close-to-zero marginal cost reproducibility of digital services (Coveri, Cozza, and Guarascio 2022). This is lavishly rewarded by financial markets, with the capitalisation 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 capitalisation further accelerates their growth, providing additional resources to invest, selectively, in R&D and M&A, which are crucial to maintain control (and technological primacy) in relevant fields such as cloud computing and AI (Rikap and Lundvall 2021; Fanti, Guarascio, and Moggi 2022). Even in this case, though, contradictions and conflicts are in order.

As the Internet becomes global, platforms augment their ability to control data, digital technologies and related infrastructures (Rikap and Lundvall 2021), as well as the new media where a large share of the public opinion is formed (Culpepper and Thelen 2020). This has significant consequences for the state-corporation nexus. First, platforms become indispensable partners in the production of public goods (e.g., the digitisation 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 if compared to previous TNCs (Ietto-Gillies 2021) as one of the peculiar domains under their control (e.g., social media) can determine whether political organisations will succeed or die.[7] 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 and abroad (see the next Section).

Such blurring boundaries and, most notably, the close connection with the security and military apparatuses make platforms the key players in the confrontation between China and the US, a confrontation that is being largely played out in the technological field (Rikap and Lundvall 2021). Indeed, China is home to the largest non-US digital platforms with a global scale — e.g., Alibaba, ByteDance, Tencent. They are the most powerful challenge to US technological (and, hence, military) supremacy (UNCTAD 2019; Hötte et al. 2023; Kissinger and Allison 2023). For 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 this confrontation, Rolf and Schindler (2023) argue that both the US and China leverage their domestic platforms to secure the control of data and extend their economic and military projection overseas.

## 3. Mutual Dependence and The Digital Platforms-Military Nexus

More than 100 years after Hobson's seminal contribution (1902), digital platforms are vindicating some of the key arguments of the theory of imperialism. Like the cartels operating at the beginning of the 20th century, they are a key driver of capitalistic accumulation (generating a substantial share of output and employment), financialisation (the growth of platforms is driven, to a significant extent, by their ability to attract ever

[7]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

larger shares of financial capital), and internationalisation (taking advantage of the global and ubiquitous nature of the Internet, platforms have expanded their presence across countries and sectors in an extremely short amount of time). Just like the corporations that, according to Lenin (1917 [1963]), gave rise to a 'new stage of capitalism', platforms are contributing to an unprecedented concentration of economic power, as their capitalisation is now worth more than the GDP of large economies like Germany or Japan (Coveri, Cozza, and Guarascio 2022).

Yet, the power of platforms is also linked to the control of knowledge, technologies and infrastructures that are essential to dominate the technological frontier, particularly in the digital domain (Rikap and Lundvall 2021). This brings back to the fore another key literature strand that has developed the theories of imperialism and shed light on the systemic role of the 20th century TNC: the MC theory (Baran and Sweezy 1966). Reinforcing a process already evidenced in the history of state-TNCs relationships, platforms' strategic interests tend to overlap with those of their home nation state (Hymer 1972). On the one hand, governments would hardly damage entities generating a substantial share of national income[8] and providing other firms with goods and services that are essential to carry out their economic activity.[9] On the other hand, platforms are often reliant on their home governments 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 organisations' struggles; on this point see also Balcet and Ietto-Gillies (2020)) and external conflicts (e.g., settling disputes with foreign governments or corporations), and support R&D projects characterised by radical uncertainty (Mazzucato 2018).

This does not rule out contradictions and conflicts, though. The growing techno-economic power of platforms gives rise to social costs (i.e., wage inequality, labour market fragmentation and precarity, competitive pressure on small — and medium-size enterprises relying on platforms to access digital marketplaces, increasing housing prices in cities whereby the presence of platforms such as Airbnb is substantial) and, therefore, to political reactions that governments attempt addressing by relying on specific policies (e.g., antitrust measures, fines, regulations restricting the access to personal data) aimed at reducing such power. Platforms, in turn, can strategically use, in addition to the classic tools aimed at conditioning government activity (e.g., lobbying), the digital infrastructures they control (e.g., social media) to secure the goodwill of the incumbent government; and/or to 'arbitrage' between political coalitions and favour those most aligned with their strategies. Furthermore, platforms may take advantage of their systemic relevance to resist 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).

[8]As of 8 July 2024, the three major US-based digital corporations — i.e., Alphabet, Amazon and Meta — represented close to $6 trillion in market value. Data retrieved from https://companiesmarketcap.com/internet/largest-internet-companies-by-market-cap/.

[9]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'.

In this tangled context, the military sector is the domain where the boundaries between state and TNCs may become blurred (Pianta 1989; Foster and McChesney 2014; Roland 2021). In this specific regard, digital platforms showcase some important discontinuities with respect to traditional military contractors. Like traditional defence contractors, digital platforms are a key partner of the military sector in designing, developing, and deploying technologies that are key to prevailing on today's battlefields. However, traditional defence contractors tend to be fundamentally tied to public demand flows stemming from the military sector and, therefore, characterised by a narrower strategic and organisational set-up. Conversely, the key technologies (e.g., cloud, AI) that platforms provide to the military sector are ubiquitous in civilian/commercial spheres, providing platforms with the essential opportunities to foster the development of incremental innovations. Therefore, platforms are more strategic partners than traditional contractors and, compared to the latter, are characterised by extreme flexibility, operating (and learning) in areas which can be far away from the military domain. No less relevant, while traditional contractors are heavily dependent on public demand for growth and profit accumulation, platforms gain the largest share of their profits from their business activities in the civil sphere. On the one hand, this gives platforms higher bargaining power vis-à-vis public procurers. On the other hand, reinforcing their relationships with military agencies is an essential strategy for them to strengthen their role as exclusive providers of (dual) technologies and services, so that their data-based and infrastructural power has no reason to be seriously challenged.

As we shall document, these factors make platforms crucial partners of the military sector. The vital resources they control (and produce), i.e., data and the technologies (e.g., AI) related to it, are vital for prevailing in contemporary conflicts. Likewise, the innovation ecosystems that platforms dominate are a fundamental source of incremental innovations, including in fields related to security and military applications (Franco et al. 2023). This strengthens mutual dependence, showing both elements of continuity and of discontinuity with respect to what Baran and Sweezy (1966) and their followers documented regarding 20th century TNCs. In what follows, we illustrate the three main drivers shaping the mutual dependency between platforms and the military sector.

### 3.1. Originary Linkage

An 'originary linkage' binds digital platforms and the military sector. During the 20th and, even more so, the 21st century, most of the breakthroughs giving rise to new industries and technological paradigms have been linked to military programmes (Polanyi 1944). 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.

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), which 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 group 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, Alphabet (former Google) and Facebook, together with companies such as Apple and Microsoft[12] that in 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., Alphabet), social networks (e.g., Meta former Facebook), 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). Such an originary linkage never fades away completely, though: even when the industries borne as a result of military-related R&D become mostly oriented towards private demand and civil purposes. 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

[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 proven 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 and Lundvall 2021), while the ongoing 'chip war' testifies to how intense the competition in this area has become (Miller 2022).

[12]Note that, although normally included among the Big Tech, corporations such as Apple and Microsoft predated the advent of what are currently defined platforms by playing a key role in traditional IT sectors, such as hardware and software industries, since the 1980s.

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 (González 2023), when resources and strategic direction are needed to push the technological frontier forward, especially when it comes to dual technologies with relevant security implications. As technological and geo-strategic conditions require it, the originary linkage is revitalised and, with it, the integration of state-corporation strategies.

### 3.2. 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 (Zikusoka 2024). Cyber-attacks and actions aimed at preventing them are becoming a matter of life or death during armed conflicts (Flournoy 2023). Likewise, digital technologies are essential to pursue security and intelligence activities (Brayne 2020), both at home and abroad (Burns 2024). 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, this frontier is dominated by few global (US and Chinese) platforms (see, among others, Kemmerling and Trampusch 2022). The latter monopolise key assets (i.e., servers, cloud infrastructures, submarine cables) (Gjesvik 2023), hold the majoritarian share of digital patents (Fanti, Guarascio, and Moggi 2022; Maslej et al. 2023) and are the locus for most of the formal and tacit knowledge — essential to move forward along technological trajectories (Dosi 1982) — is developed (Rikap and Lundvall 2021).[13]

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.[14] 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, the 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

[13]As for the growing ownership of undersea cables by digital platforms, especially Amazon, Google and Facebook, see Seal, T., 'The Undersea Cable Market Is Booming Again, This Time Funded by Big Tech', *Bloomberg,* 14 March 2019, available at: https://www.bloomberg.com/news/articles/2019-03-14/undersea-cables-are-no-longer-underwater-as-fiber-booms-again. Last access: 10 June 2024.

[14]See: https://aws.amazon.com/it/blogs/iot/increase-military-readiness-with-aws-iot-for-defense-and-national-security/. Last access: 10 June 2024.

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 the platforms' position vis-à-vis both potential competitors as well as governments (Coveri, Cozza, and Guarascio 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 and Lundvall 2021; Gawer 2022; Jacobides, Cennamo, and Gawer 2024). By governing knowledge co-creation processes and exploiting the modular structure of digital ecosystems, platforms benefit from the decentralised nature of digital innovation while preserving their economic and technological power. Similar dynamics apply to military-related supply chains. To digitise processes and products (including weapons), traditional defence contractors (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 (see Wong and Younossi 2023).[15]

The third driver of dependence concerns skills and training activities. In high-tech industries, competencies tend to be complex, idiosyncratic, technology- and organisation-specific (Dosi and Marengo 2000). 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, and other firms, and the government, on the other (Flournoy 2023). This is due to the career prospects the former can offer and the 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 the related training activities, as the latter tend to monopolise 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 strategic projects. As documented by Lundvall and Rikap (2022), such a role is often formalised in public bodies of acknowledged importance, including those aimed at designing military-related frontier technologies (e.g., AI).

[15]Several collaborations between digital platforms and traditional defence contractors have been released in the last years, with the former providing key technologies and infrastructures to the latter. In particular, both Amazon and Microsoft entered into agreements with Lockheed Martin, Raytheon Technologies, Halliburton and BAE Systems for the provision of cloud services and other military-related technologies, although public details on these contracts are scant. See, e.g., aws.amazon.com/blogs/publicsector/accelerating-mission-critical-development-for-national-defense/; and defensemirror.com/news/33110/Lockheed_Martin_to_Operate_Inside_Microsoft_Azure_s__Secret_-Cloud (last access: 15 June 2024). However, the relationship between platforms and traditional defence contractors is significantly complex, and the degree of cooperation, technological dependence and conflict can vary greatly depending on the platform considered, the technology or the service at stake, as well as the characteristics of the contractor involved in the relationship. The investigation of such a key relationship is an important area of research that will require in-depth study in the future.

### 3.3. 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 organisations. 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 of) 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 try 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 hand, 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,[16] while Facebook and Twitter have intervened to stop disinformation campaigns by taking down networks of hijacked computer devices used to perform cyberattacks.[17] This inevitably results in these private corporations assuming a prominent role in assuring 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

[16]On this point, see: https://www.nytimes.com/2023/07/11/us/politics/china-hack-us-government-microsoft.html; and https://www.microsoft.com/en-us/security/business/security-intelligence-report

[17]On this point, see: www.npr.org/2022/09/27/1125217316/facebook-takes-down-russian-network-impersonating-european-news-outlets; www.intelligence.senate.gov/sites/default/files/documents/os-jdorsey-090518.pdf

whitelisting many social profiles. This network has been used by the DoD to directly influence public opinion in countries involved in military conflicts such as Yemen, Syria, Iraq, Kuwait and beyond.[18] 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.

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 and 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 has 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).[19]

More broadly, by partnering with digital corporations that control critical technologies and infrastructures — e.g., cloud (Rikap and Lundvall 2022), AI (Fanti, Guarascio, and Moggi 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) calls '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. (Kwet 2019, p. 4)

In other words, being the exclusive suppliers of services for both business growth and 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 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).

[18]On this point, see https://theintercept.com/2022/12/20/twitter-dod-us-military-accounts/

[19]In the European case, there is substantial dependence on US-based platforms for most advanced digital services (e.g., cloud, AI). There are no European platforms comparable to the US and Chinese giants, and most of the infrastructure and technologies are concentrated in the two poles (Guarascio et al. 2024).

## 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 analyse the evolution of the US Department of Defense (DoD) procurement contracts, showing the growing relevance of platforms as DoD procures. 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 (King and Shull 2020), but are also characterised by high complexity, cumulativeness and strong complementarity with their idiosyncratic capabilities (Mowery 2010). Although this evidence cannot provide definitive proof of the existence of a 'mutual dependence' between platforms and military apparatuses, we believe that documenting the latter's growing reliance on the former for the development (and active management) of critical technologies and infrastructure (e.g., the AWS Cloud Computing for the US Department of Defense) is especially suggestive of the increasingly tighter relationship binding US defence agencies to platform giants.

Moreover, we document the 'revolving doors' mechanism 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 analyse the available evidence on the active participation of key US-based platforms in the Russo-Ukrainian war.

### *4.1. 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 (per cent) 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 per cent in the second half of the 1990s and fluctuating around 45 per cent in the first two decades of the 2000s (Mowery 2009, 2010).

Further confirming this pattern, the US DoD's weapon systems acquisition funds requested for fiscal year (FY) 2024 $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 2000–22. These figures highlight

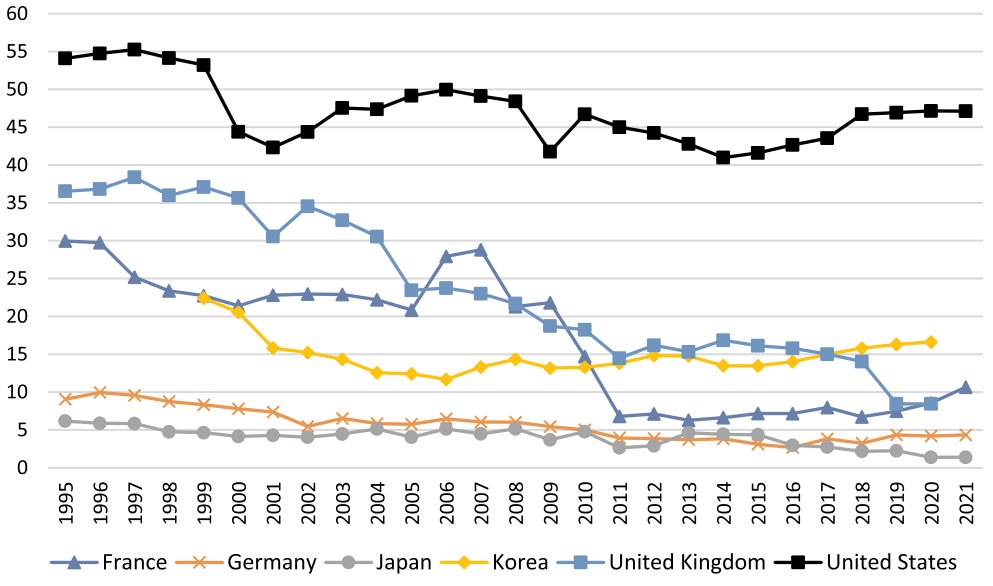


**Figure 1.** GBARD for Defence (% of total GBARD), 1995–2021. Source: authors' elaboration based on OECD data. Government budget allocations for R&D (GBARD) for Defence (2015 US Dollar Millions, constant prices and PPPs).

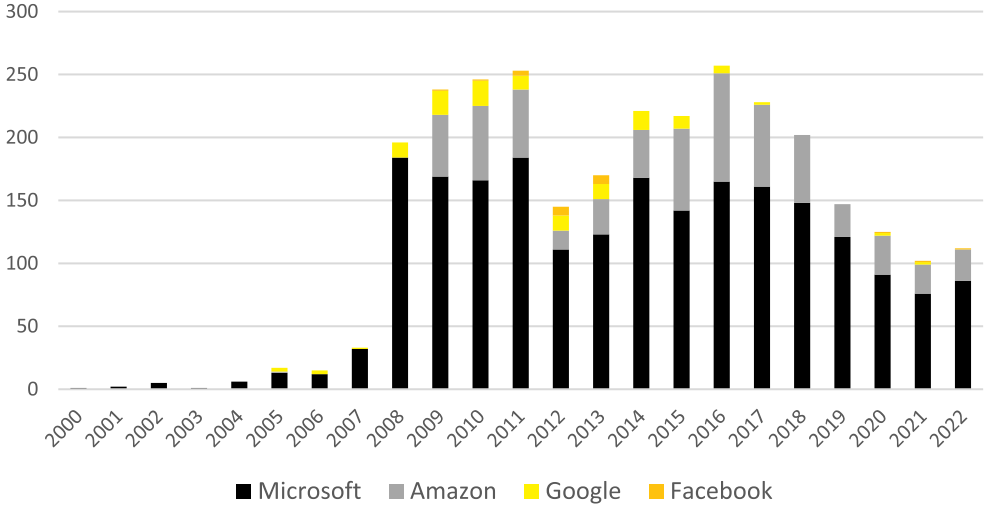


**Figure 2.** Number of Amazon, Google, Facebook and Microsoft's contracts with all US federal agencies, 2000–22. Source: authors' elaboration based on *USAspending.gov* data.

that a major acceleration in the total number of contracts awarded to digital corporations has occurred since 2008. From 2008 to 2018, digital platforms were 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 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 grew rather steadily from 2008 to 2022. Microsoft reports by far the greatest 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 per cent of the value of all US agencies' contracts stipulated with Microsoft were awarded by the DoD. Added to this is the value of subcontracts, i.e., contracts awarded by US federal agencies to recipients who subcontracted part of the service to a platform. 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 per cent of the overall value of subcontracts).

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 was awarded by the DoD (equal to little less than 40 per cent of the value of all contracts awarded to Amazon by US federal agencies). Interestingly, the value of the overall subcontracts awarded to Amazon by all US federal agencies is equal to about $450 million over the whole period, of which slightly more than $200 million was (indirectly) awarded by the DoD (45 per cent of the overall value of subcontracts). It follows that, for this platform, the value of subcontracts is greater than the value of the contracts, and together they amount to nearly $600 million (of which just under half were awarded by DoD).

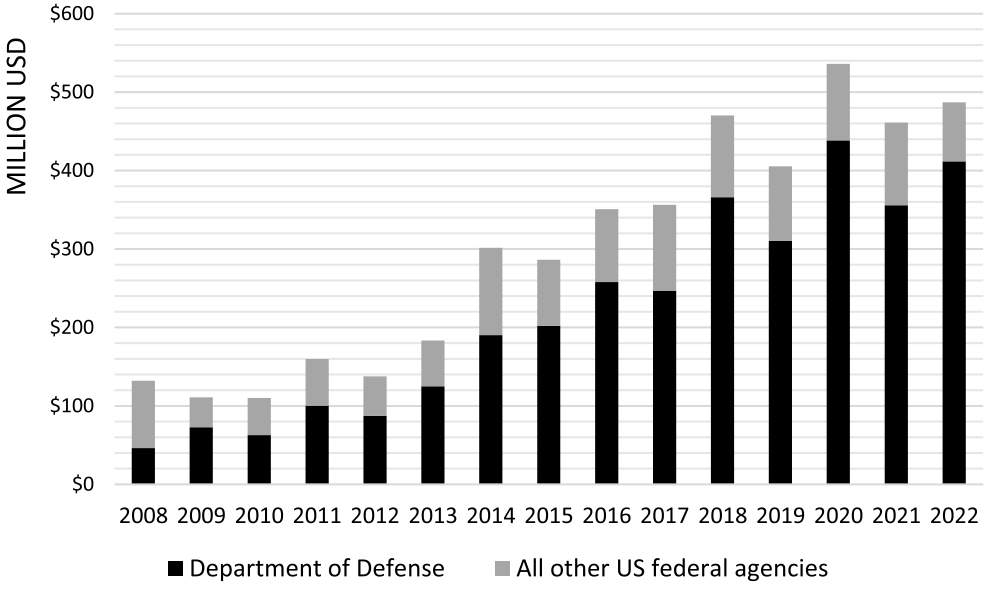


**Figure 3.** Total value of Amazon, Google, Facebook and Microsoft's contracts with the US Department of Defense and other US federal agencies, 2008–22. Source: authors' elaboration based on *USAspending.gov* data.

Consistently with Figure 2, and in line with the evidence provided by Maaser and Verlaan (2022), we find that the overall value of the contracts and subcontracts awarded to Alphabet and Facebook is relatively low, amounting to about $59 and $3 million, respectively.

### 4.2. 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. 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 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 for 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.[20] 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.[21]

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

[20]On this point, see: https://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/. Last access: July 15 2023

[21]On this point, 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.

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

| 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'[23] | Cloud | Cloud services centralised for 17 intelligence agencies (Commercial Cloud Enterprise) |
| 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) |
| 2022 — DoN/ DoD | Amazon | 724 million | Cloud | Cloud services to process and store data for critical missions |
| 2023 — SSC/ DoD | Microsoft | 19.8 million | Cloud-based space simulation (viewable with Microsoft HoloLens headsets) | Space simulator aimed at gaining situational awareness and acting faster than adversaries |
| 2024 — DoD | Amazon | 22 million | Cloud | Cloud services for the Army department of the US Special Operations Command |

Source: authors' elaboration on press sources. CIA stands for Central Intelligence Agency, NSA for National Security Agency, DoD for Department of Defense, DoN for Department of the Navy, SSC for Space Systems Command. NA stands for not available.

workloads classified as 'top secret', i.e., the 'Azure Government Top Secret' in 2021, following the announcement of 'Azure Government Secret' in 2017.[22] 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.[24] In April 2022, the NSA awarded a $10 billion cloud computing contract to AWS. This contract, called 'Wild and Stormy'

[22]On this point, 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.

[23]See https://www.nextgov.com/modernization/2019/04/cia-considering-cloud-contract-worth-tens-billions/156190/. Last access: 10 February 2024.

[24]On this point, see https://gcn.com/cloud-infrastructure/2020/11/cia-awards-massive-cloud-contract/315771/. Last access: July 15 2023.

(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.[25] Later that year, Amazon was awarded an additional contract, worth $724 million, for providing the Department of the Navy with access to AWS commercial cloud services.[26]

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. A few months later, GPS announced the provision of Google's workspace to 250.000 US Army personnel. 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.[27] 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.'[28]

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 AI and ML technologies for the US 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).'[29] This follows the inclusion of AWS among the companies allowed to compete for 'Indefinite Delivery/Indefinite Quantity' contracts, which give these firms the opportunity to be awarded with $950 million over five years for developing new digital capabilities for ABMS.[30] 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.[31] 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 centres with built-in AWS infrastructure to store and analyse data in real-time 'to

[25]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

[26]On this contract, see: https://defensescoop.com/2022/12/23/aws-wins-724m-contract-providing-navy-access-to-commercial-cloud-environment/ (last access: 20 June 2024).

[27]On this point, see: https://edition.cnn.com/2022/12/08/tech/pentagon-cloud-contract-big-tech/index.html. Last access: 8 September 2023.

[28]For a description, see https://aws.amazon.com/blogs/publicsector/aws-selected-for-u-s-department-of-defense-joint-warfighting-cloud-capability-contract/. Last access: 9 January 2024.

[29]For a detailed description, see: https://aws.amazon.com/it/blogs/publicsector/bringing-cloud-air-force-speed-of-mission-need/. Last access: 8 September 2023.

[30]On this point, see: https://www.af.mil/News/Article-Display/Article/2359938/abms-signs-more-companies-post-onramp/. Last access: 8 September 2023.

[31]On this point, see: https://aws.amazon.com/it/blogs/publicsector/aws-supports-development-u-s-armys-first-enduring-tactical-cloud-environment/. Last access: 2 December 2023.

gain military advantage in the most isolated environments'[32] — and of the AWS Snowblade, a device designed to compute, store, and handle data for enabling defence warfighters to complete missions in highly risky locations.[33] The collaboration between Amazon and the DoD was further bolstered in early 2024, when AWS was awarded a $22-million contract to provide cloud services to the Army department of the US Special Operations Command.[34]

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;[35] and was followed in December 2023 by a $19.8-million contract for Microsoft to provide a cloud-based space simulator to the US Space Systems Command (SCC), viewable through Microsoft HoloLens headsets.[36]

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.[37] Following this protest, Google effectively abandoned the Maven project in early 2019,[38] being replaced by Microsoft, which received a $30-million contract in 2019, and AWS, which was awarded a $20-million contract in 2020.[39] 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 Project Maven was given by the DoD in 2022.[40] As for Microsoft, in August 2022 the US Army integrated the breakthrough technology that it had designed for Stryker armoured vehicles in order to provide warfighters with enhanced

[32]On this point, see: https://aws.amazon.com/it/blogs/publicsector/announcing-aws-modular-data-center-u-s-department-defense-joint-warfighting-cloud-capability/. Last access: 13 January 2024.
[33]On this point, see: https://aws.amazon.com/about-aws/whats-new/2023/06/aws-snowblade-us-defense-jwcc-customers/. Last access: 10 January 2024.
[34]On this contract, see: https://www.defense.gov/News/Contracts/Contract/Article/3786556/. Last access: 5 July 2024.
[35]On this point, see: https://www.cnbc.com/2021/03/31/microsoft-wins-contract-to-make-modified-hololens-for-us-army.html. Last access: 8 September 2023.
[36]On this contract, see: https://defensescoop.com/2024/01/08/space-force-i3e-contract-microsoft/. Last access: 25 February 2024.
[37]On this point, see: https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html. Last access: 8 September 2023.
[38]On this point, see: https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html. Last access: 8 September 2023.
[39]On this point, 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/. Last access: 8 September 2023.
[40]On this point, see: '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.

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 Defense 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 Defense 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 organisations across Europe.[41]

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). This is in line with the Pentagon's more general long-term commitment to accelerate the adoption of commercially developed AI and cloud technologies for military use (González 2023). 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 speeding up military procurement. The goal was to create a 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 (Kaplan 2016). 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.[42]

### 4.3. 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). As is known, revolving doors between the US defence apparatus and the private military industry are a long-term common practice (Brunton 1988; Etzion and Davis 2008; Duncan and Coyne 2015). Accordingly, this mechanism stands out as an element of continuity with respect to the traditional US military-industrial complex. This practice is nonetheless worth documenting when exploring the platforms-military nexus, as it represents a

[41]On this point, see: https://aws.amazon.com/it/blogs/publicsector/aws-launches-2023-european-defence-accelerator-for-startups/

[42]On this point, 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.

further dimension of the integration between digital companies and government defence agencies.

On the one hand, the moving of personnel from platforms to military agencies 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.[43] 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,[44] Schmidt has served as chairman of the Defense Innovation Advisory (DIA) Board and co-chairman of the National Security Commission on AI (NSCAI), i.e., two government advisory boards aimed at jump-starting DoD's technological innovation to counter the emerging technological power of China. Nonetheless, Schmidt relied on his own venture capital to invest in defence start-ups, thus becoming an important actor on 'both sides of the table' at the same time.[45]

On the other hand, the experience and contacts obtained 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 procurement, and played a key role in formulating the ethical principles for the Joint Artificial Intelligence Center.[46]

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

[43]On this point, 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.

[44]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 and Russia's technological advances (Gentile et al. 2021).

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

[46]On this point, 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.

$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's oversight.[47]

The 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.[48] 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.[49]

### 4.4. Digital Platforms Go to War

Further evidence is provided by the active participation of platforms in warfare activities. A case in point is the dreadful war in Ukraine, where major US-based platforms have assumed, since the war's very early stages, a direct role in the deployment of critical information-related infrastructures and technologies (Coveri, Cozza, and Guarascio 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.[50] Notably, in September 2022 the sudden shutdown of Starlink jeopardised a decisive military operation targeting Russian warships near the coast of Crimea. SpaceX owner and CEO Elon Musk recently stated that the shutdown was his deliberate decision, due to the fear that Russia might respond to the Ukrainian attack with nuclear weapons. Shortly after these events, Musk finalised the acquisition of another key digital corporation, Twitter, and entered into negotiations with the US government (as well as its European allies) regarding the financing of Starlink.[51] A month later, Musk was reported (although he denied it) to have held a direct channel with Putin discussing his own 'peace plan' for Ukraine.[52]

[47]On this point, 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.

[48]On this point, 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.

[49]On this point, 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.

[50]On this point, 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.

[51]On 1 June 2023, it was disclosed that Elon Musk's SpaceX was awarded a contract by the 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. Last access: 21 December 2023.

[52]On this point, see: https://fortune.com/2022/10/11/elon-musk-ian-bremmer-putin-russia-ukraine/. Last access: 21 December 2023.

Two elements stand out here: first, the crucial role played by a private corporation, whose activity is theoretically intended for the civil sphere, in a war, providing SpaceX with a stronger bargaining 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 Russo-Ukrainian War, however. AWS disclosed that, as early as 24 February 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.'[53] Since then, 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. 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 of technology 'to ensure that government agencies, critical infrastructure and other sectors in Ukraine can continue to serve citizens through the Microsoft Cloud';[54] it also took legal and technical action to withdraw Internet launch points used by the Russian army for its attacks (Fox and Probasco 2022). 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.[55]

Overall, platforms' active participation in warfare activities is another element that may help explain the mutual dependence. On the one hand, platforms' direct involvement in war scenarios provides them with a unique opportunity to test their technologies on the battleground, check their operability and security, and adapt them accordingly. Testing technologies and military-related infrastructures in real-world battlefields enables platforms to improve their technological capabilities further, in a way that could not be feasible otherwise. In other terms, battlefields become 'military technologies

[53]On this point, see: https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future. Last access: 21 December 2023.

[54]On this point, 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.

[55]The Palestinian-Israeli conflict is another war scenario involving digital platforms. Amazon and Google were awarded a $1.2-billion contract by the Israeli government for the provision of AI and cloud services aimed at facial recognition and object tracking for security and military purposes. The contract, called 'Project Nimbus', was announced by the Israeli government in April 2021. In early 2024, after Israel's military response to the terrorist attack by Hamas on 7 October 2023, *The Intercept* stated that Google had been negotiating an extension of the partnership with the Israeli Ministry of Defense to provide additional cloud technologies. See https://theintercept.com/2024/05/01/google-amazon-nimbus-israel-weapons-arms-gaza/. About 50 Google engineers were fired for opposing Project Nimbus. (similar protests took place in Amazon). See https://www.theguardian.com/technology/2024/apr/27/google-project-nimbus-israel (last access: 15 June 2024).

labs' for platforms.[56] On the other hand, 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 platforms' bargaining power may grow as they increase the amount of critical information under their control and the exclusivity of the technology-specific capabilities they develop. However, in this case the platforms-state nexus is not free of contradictions. In fact, being involved in close relationships with military apparatuses — which operate with logic that differs from that of standard market relationships — exposes platforms to risks and may reduce their strategic and operational flexibility (Pianta 1989). No less relevant is the integration between platforms and the military agencies that could be threatened by conflicts between top managers intending to meet DoD's demand and by highly skilled personnel — e.g., engineers and software developers — that may consider the development of war-related technologies ethically unacceptable (González 2023).

## 5. Conclusions

According to theories of imperialism and Monopoly Capital, military expenditure and warfare are the results 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 hand, as an intrinsic feature of capitalist accumulation and the driving force of inter-imperialist conflicts.

Building on these theories, in this work we have 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 'eyes and ears' (both at home and abroad). In addition to their systemic relevance, which allows 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 augmented, 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 means, a demand-pull innovation driver and 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 procures, 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.

[56]From this perspective, the war in Ukraine is a case in point. See Fox and Probasco (2022) and Bergengruen (2024).

Remarkably enough, these corporations develop and deploy the same dual technologies that enable them to dominate the digital market and 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 emphasised the convergence between corporate and state strategies, these strategies 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 shows the dark side of 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'. Yet, recalling Freeman (1991), it is important to go beyond simplistic views and acknowledge the contribution to the 'politicization of technology' made by Luddites. Rather than an irrational rejection of technological change as such, their action should be interpreted as the need to classify technologies according to their social acceptability. In the era of digital platforms, though, such a critical approach should not (or not solely) be driven by the fear of mass technological unemployment and related inequalities, 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.

Some limitations of this work should also be acknowledged. First, it would be worthwhile to delve deeper into comparing and contrasting the nature of the big TNCs of the 20th century and the large digital platforms that have emerged over the past twenty or thirty years. Although we have outlined some important distinctions among them, we have not delved into the differences concerning their peculiar relationship with the state in general and with the military apparatus in particular. Such an analysis is required to offer further evidence supporting the 'mutual dependence' hypothesis we put forward in this work. Second, the complex collaborations between digital platforms and traditional defence contractors require more in-depth investigation. Exploring the role played by digital platforms in the value chain of the military industry, as well as the potential synergies and conflicts arising between platform giants, traditional contractors and defence start-ups would further illuminate the intricate features of the emerging 'digital-military complex'. These represent promising avenues for future research.

## Acknowledgements

We greatly thank two anonymous reviewers for their valuable comments on an earlier version of the manuscript. We also thank participants to the Rentier Capitalism Workshop held at City University of London in November 2022, the Advanced Course on Innovation, Growth, International Production held at Sapienza University of Rome in May 2023, the SASE conference in Rio de Janeiro in July 2023, the EAEPE conference held in Leeds and the EuroMemorandum conference held at University of Naples 'Parthenope' in September 2023, the Historical Materialism conference held at SOAS University of London in November 2023, the Post-Keynesian Conference held in Lille in December 2023, the ASTRIL conference held at Roma Tre University in January 2024, and the workshop held at the Nexa Center for Internet and Society at the Polytechnic of Turin in February 2024. The usual disclaimer applies.

## Disclosure Statement

No potential conflict of interest was reported by the author(s).

## ORCID

*Andrea Coveri* http://orcid.org/0000-0002-5891-7407
*Claudio Cozza* http://orcid.org/0000-0001-7407-3497
*Dario Guarascio* http://orcid.org/0000-0002-2748-6472

## References

Arrighi, G. 1978. *The Geometry of Imperialism: The Limits of Hobson's Paradigm*. London: New Left Books.

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*. New York: Monthly Review Press.

Beaumier, G., and K. Kalomeni. 2022. 'Ruling Through Technology: Politicizing Blockchain Services.' *Review of International Political Economy* 29 (6): 2135–2158.

Bergengruen, V. 2024. 'How Tech Giants Turned Ukraine Into an AI War Lab.' *Time Magazine*, February 8. Accessed June 10, 2024. https://time.com/6691662/ai-ukraine-war-palantir/.

Brayne, S. 2020. *Predict and Surveil: Data, Discretion, and the Future of Policing*. Oxford: Oxford University Press.

Brunton, B. G. 1988. 'Institutional Origins of the Military-Industrial Complex.' *Journal of Economic Issues* 22 (2): 599–606.

Burns, W. J. 2024. 'Spycraft and Statecraft: Transforming the CIA for an Age of Competition.' *Foreign Affairs*, January 30. Accessed June 10, 2024. https://www.foreignaffairs.com/united-states/cia-spycraft-and-statecraft-william-burns.

Calvino, F., C. Criscuolo, H. Dernis, and L. Samek. 2023. 'What Technologies are at the Core of AI? An Exploration based on Patent Data.' *OECD Artificial Intelligence Papers*, No. 6. Paris: OECD Publishing.

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*. https://www.socialeurope.eu/war-in-the-time-of-digital-platforms.
Cowling, K. 1982. *Monopoly Capitalism*. Basingstoke: Macmillan.
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*. New York: 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*. Bristol: Bristol University Press.
DoD. 2023. *Fiscal year 2024 Program Acquisition Cost by Weapon System*. United States Department of Defense. https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2024/FY2024_Weapons.pdf.
Dosi, G. 1982. 'Technological Paradigms and Technological Trajectories: A Suggested Interpretation of the Determinants and Directions of Technical Change.' *Research Policy* 11 (3): 147–162.
Dosi, G. 1984. *Technical Change and Industrial Transformation: The Theory and an Application to the Semiconductor Industry*. Basingstoke: Macmillan.
Dosi, G., and L. Marengo. 2000. 'Some Elements of an Evolutionary Theory of Organizational Competences.' In *Innovation, Organization and Economic Dynamics: Selected Essays*, edited by G. Dosi. Cheltenham: Edward Elgar.
Duncan, T. K., and C. J. Coyne. 2015. 'The Revolving Door and the Entrenchment of the Permanent War Economy.' *Peace Economics, Peace Science and Public Policy* 21 (3): 391–413.
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.
Etzion, D., and G. F. Davis. 2008. 'Revolving Doors? A Network Analysis of Corporate Officers and U.S. Government Officials.' *Journal of Management Inquiry* 17 (3): 157–161.
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.
Flournoy, M. A. 2023. 'AI Is Already at War: How Artificial Intelligence Will Transform the Military.' *Foreign Affairs*, October 24. Accessed June 10, 2024. https://www.foreignaffairs.com/united-states/ai-already-war-flournoy.
Foster, J. B. 2014. *The Theory of Monopoly Capitalism*. New York: Monthly Review Press.
Foster, J. B., and R. McChesney. 2014. 'Surveillance Capitalism.' *Monthly Review* 66 (3): 1–31.
Fox, C. H., and E. S. Probasco. 2022. 'Big Tech Goes to War. To Help Ukraine, Washington and Silicon Valley Must Work Together.' *Foreign Affairs*, October 19. Accessed June 10, 2024. https://www.foreignaffairs.com/ukraine/big-tech-goes-war.
Franco, S. F., J. M. Graña, D. Flacher, and C. Rikap. 2023. 'Producing and Using Artificial Intelligence: What Can Europe Learn from Siemens's Experience?' *Competition & Change* 27 (2): 302–331.
Freeman, C. 1991. 'Innovation, Changes of Techno-Economic Paradigm and Biological Analogies in Economics.' *Revue Économique* 42 (2): 211–232.
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*. Princeton: 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*. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/research_reports/RRA454-1.html.

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

González, R. J. 2023. 'Militarising Big Tech. The Rise of Silicon Valley's Digital Defence Industry.' *Transnational Institute* 1–14. https://www.tni.org/en/article/militarising-big-tech.

Greenstein, S. 2015. *How the Internet Became Commercial: Innovation, Privatization, and the Birth of a New Network*. Princeton: 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*. London: Bloomsbury Publishing.

Guarascio, D., J. Reljic, G. Cucignatto, G. Celi, and A. Simonazzi. 2024. 'Between Scylla and Charybdis: Long-Term Drivers of the EU Structural Vulnerability.' *Review of Keynesian Economics. Forthcoming*.

Hilferding, R. 1910. *Das Finanzkapital. Eine Studie über die jüngste Entwicklung des Kapitalismus*. Vienna: 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: General Purpose Technology and Concentration of Actors*. INET Oxford Working Paper No. 2023-09.

Hymer, S. H. 1960 [1976]. *The International Operations of National Firms, a Study of Direct Foreign Investment*. PhD thesis, Massachusetts Institute of Technology.

Hymer, S. H. 1970. 'The Efficiency (Contradictions) of Multinational Corporations.' *The American Economic Review* 60 (2): 441–448.

Hymer, S. H. 1972. 'The Internationalization of Capital.' *Journal of Economic Issues* 6 (1): 91–111.

Ietto-Gillies, G. 2002. *Transnational Corporations: Fragmentation Amidst Integration*. London: Routledge.

Ietto-Gillies, G. 2012. *Transnational Corporations and International Production: Concepts, Theories and Effects*. Cheltenham: Edward Elgar.

Ietto-Gillies, G. 2021. 'Transnationality in the XXI Century. Concept and Indicators.' *Critical Perspectives on International Business* 18 (3): 338–361.

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*. New York: Little, Brown and Company.

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*, edited by R. van Tulder, A. Verbeke, and L. Piscitello. Leeds: Emerald Publishing Ltd.

Johnson, J. 2019. 'Artificial Intelligence & Future Warfare: Implications for International Security.' *Defense & Security Analysis* 35 (2): 147–169.

Kaplan, F. 2016. 'The Pentagon's Innovation Experiment.' *MIT Technology Review*, December 19. Accessed September 8, 2023. https://www.technologyreview.com/2016/12/19/155246/the-pentagons-innovation-experiment/.

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* 21 (4): 1851–1876.

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.
King, M., and A. Shull. 2020. 'Introduction: How Can Policy Makers Predict the Unpredictable?' CIGI Essay Series on *Modern Conflict and Artificial Intelligence*, November. https://www.cigionline.org/modern-conflict-and-artificial-intelligence/.
Kissinger, H. A., and G. Allison. 2023. 'The Path to AI Arms Control: America and China Must Work Together to Avert Catastrophe.' *Foreign Affairs*, October 13. Accessed June 10, 2024. https://www.foreignaffairs.com/united-states/henry-kissinger-path-artificial-intelligence-arms-control.
Kurz, M. 2023. *The Market Power of Technology. Understanding the Second Gilded Age*. New York: 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. 1917 [1963]. *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. 1913 [2003]. *The Accumulation of Capital*. London: Routledge.
Maaser, L., and S. Verlaan. 2022. 'Big Tech Goes to War.' In *Studien*, Vol. 5, 1–31. Berlin: Rosa-Luxemburg-Stiftung.
Marx, K. 1867 [2004]. *Capital: Volume I*. London: Penguin.
Marx, K., and F. Engels. 1848 [1967]. *The Communist Manifesto*. London: Penguin.
Maslej, N., L. Fattorini, E. Brynjolfsson, J. Etchemendy, K. Ligett, T. Lyons, J. Manyika, et al. 2023. *Artificial Intelligence Index Report 2023*. Stanford, CA: AI Index Steering Committee, Institute for Human-Centered AI, Stanford University.
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*. London: Simon and Schuster.
Mowery, D. C. 2009. 'National Security and National Innovation Systems.' *Journal of Technology Transfer* 34 (5): 455–473.
Mowery, D. C. 2010. 'Military R&D and Innovation.' In *Handbook of the Economics of Innovation*, Vol. 2, edited by B. Hall and N. Rosenberg. Amsterdam: 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*. New York: Penguin Press.
Paulson, R. 2021. *Tech Inquiry Report* 2021. Public Available Information (PAI), 1–42. https://techinquiry.org/EasyAsPAI/resources/EasyAsPAI.pdf 5.
Paulson, R. 2022. *Tech Inquiry Report* 2022. Public Available Information (PAI), 1–154. https://techinquiry.org/docs/InternationalCloud.pdf.
Pianta, M. 1989. 'High Technology Programmes: For the Military or for the Economy?' In *Making peace possible: The promise of economic conversion*, edited by L. J. Dumas and M. Thee. Oxford: Pergamon Press.
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* 46 (6): 1243–1268.
Polanyi, K. 1944. *The Great Transformation*. New York: Beacon.
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.' CITYPERC Working Paper No. 2023-03.

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. 2021. *The Digital Innovation Race: Conceptualizing the Emerging New World Order*. Cham: Palgrave Macmillan.
Rikap, C., and B-Å Lundvall. 2022. 'Big Tech, Knowledge Predation and the Implications for Development.' *Innovation and Development* 12 (3): 389–416.
Roland, A. 2021. *Delta of Power: The Military-Industrial Complex*. Baltimore: Johns Hopkins University 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* 55 (5): 1255–1280.
Roncaglia, A. 2005. *The Wealth of Ideas: A History of Economic Thought*. Cambridge, UK: Cambridge University Press.
Sawyer, M. 2022. 'Monopoly Capitalism in the Past Four Decades.' *Cambridge Journal of Economics* 46 (6): 1225–1241.
Schmid, J. 2018. 'The Diffusion of Military Technology.' *Defence and Peace Economics* 29 (6): 595–613.
Schmidt, E. 2023. 'Innovation Power. Why Technology Will Define the Future of Geopolitics.' *Foreign Affairs*, February 28. Accessed June 10, 2024. https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics.
Schumpeter, J. A. 1951. *Imperialism and Social Classes*. New York: Augustus M. Kelley, Inc.
Stiglitz, J. E. 1991. 'The Invisible Hand and Modern Welfare Economics.' In *Information, Strategy, and Public Policy*, edited by D. Vines and A. A. Stevenson. Oxford: Blackwell.
UNCTAD. 2019. *Digital Economy Report 2019: Value Creation and Capture. Implications for Developing Countries*. New York: UN Publications.
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* 46 (6): 1269–1288.
Wong, J., and O. Younossi. 2023. *Improving Defense Acquisition: Insight from Three Decades of RAND Research*. Santa Monica, CA: RAND Corporation.
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.
Zikusoka, D. 2024. 'Spying From Space: How a Surge in Satellites Will Revolutionize Intelligence.' *Foreign Affairs*, February 2. Accessed June 10, 2024. https://www.foreignaffairs.com/united-states/spying-space.
Zuboff, S. 2019. *The Age of Surveillance Capitalism*. New York: Public Affairs.

# Appendix

**Table A1.** Comparing XX century TNCs with Digital platforms.

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

Source: authors' elaboration.