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

Andrea Coveri^a, Claudio Cozza^b, Dario Guarascio^c

^aUniversity of Urbino Carlo Bo, insert, Urbino, insert, Italy ^bUniversity of Naples 'Parthenope', Via Generale Parisi 13, Naples, 80132, Italy ^cSapienza University of Rome, Via del Castro Laurenziano 9, Rome, 00161, Italy

Abstract

Building on the Monopoly Capital tradition (Baran and Sweezy, 1966), this paper sheds new light on the mutual dependence between digital corporations and governments, with particular reference to their military apparatuses. Following up on previous work (Coveri et al., 2022), we disentangle the economic, technological and institutional channels through which such mutual dependence is shaped. Moreover, we provide a quantitative and qualitative assessment of the digital platforms-military nexus. Focusing on the US, we, first, analyze the evolution of the Department of Defense (DoD) procurement contracts showing the growing relevance of platforms as DoD procurers. Second, we qualitative analyse a selection of contracts entrusting platforms to develop and manage critical technologies and infrastructures. Finally, we rely on recent information to document the direct involvement of key US-based platforms in the Ukraine war.

Keywords: Monopoly capital, war, government, digital platforms *JEL*:

"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, as cited in Hobson, 1902). The exact quote being: "Therefore I must say that, as I hope for mercy, I can have no other notion of all the other governments that I see or know, than that they are a conspiracy of the rich, who, on pretence of managing the public, only pursue their private ends, and devise all the ways and arts they can find out" (Sir Thomas More, 1516). "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).

1. Introduction

When we think about wars, or more generally about contrast of interests, we tend to isolate the two dimensions: such contrasts can be seen either as a clash of abstract human tensions (private dimension); or as a conflict of groups of individuals, typically in the form of nation-states or corporations, one against the others (thus affecting the public dimension). Following the first approach, we might highlight the psychological aspect of autocrats starting a war or also visionary entrepreneurs launching a new business, for their own abstract interest. Following the second one, we might discover the practical advantages of, as an example, a colonialist state invading new territories or of an oil 'transnational' corporation (TNC), coming from that same colonialist state, monopolising the oil extraction business in the invaded territory. However, over the centuries the relation between the public and the private interests has been described by philosophers as being much more complex and interconnected. Recently, such complexity keeps on being studied by political scientists, philosophers and social scientists: for them, as it is obvious, the economic explanation of human events such as a war is just one dimension among many others. They are not interested in highlighting the 'economic roots' of social phenomena. Vice versa, economists are more and more responsible for the *separation* of the private and public dimensions. Mainstream economic theories are still constrained by the XVIII century 'Utilitarian' perspective: markets would be the practical expression of private interests; while states would eventually concern the realisation of the public ones.

Such a perspective not only disregards great achievements of modern times philosophers (e.g., Thomas More or Adam Smith, as in our epigraph). It also completely removes the analyses made on the first period of global conflicts in contemporary history, that is about imperialism and war more than one century ago. Here, we refer to the work of Hobson (1902), who first defined the economic (material) roots of imperialistic wars and clearly showed how nation-states did not pursue the public interest, but rather that of national lobbies. And to the analysis of Lenin (1963 [1917]) who, building upon the works of Hobson and Hilferding (1908 [1923]) proposed a new definition of 'Imperialism'¹. The latter is defined 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.'

Focusing on the relationship between dominant corporations (i.e., monopolies and cartels) and the state, Lenin highlights a peculiar convergence between their respective expansionary strategies.² In this context, the capital's 'expansionary logic' - i.e., corporations relentlessly looking for new avenues to export capital, capture value and increase control over competitors, suppliers, raw materials and workers - is mirrored by the emergence of a "hierarchical ordering of multiple states under the hegemony of dominant nation-state/s" (Vasudevan, 2021). And this leads to the economic roots of war. Violence and conflicts are in fact a 'natural outcome' of nation states' activities aimed at supporting their domestic corporations to: i) open up new markets and seize new raw material sources; ii) secure trade routes and key logistics hubs; iii) prevent competitors (as well as subordinate allies) from gaining technological or trade-related competitive advantages; iv) counter the reactions of those (e.g., foreign governments, trade unions) resisting corporations' expansions.

The relationship between states and monopolies studied by Hobson, Hilferding and Lenin is however rather different from the complex network of interests linking governments and today's large TNC (e.g., large digital platforms also known as 'Big Tech') (Coveri et al., 2022). As size, scope and technological complexity of corporations grow, such relationship changes and *contradictions* may flourish (Arrighi, 1981).³ Such a growing complexity is

¹During the same period, another popular definition of Imperialism is provided by Rosa Luxemburg. According to this author, imperialism can be interpreted as the 'colonization', mostly aimed at violently exploiting human and natural resources, of what remains still open of the 'non-capitalist environment', both inside and outside the capitalist economies of her times (Kowalik, 2014)

²The overlapping between capitalists and nation states' strategies can be synthesized recalling Marx and Engels' words: 'executive of the modern state is [nothing] but a committee for managing the common affairs of the whole bourgeoisie' (Marx and Engels, 1967 [1948])

 $^{^{3}}$ There is quite an unanimous consensus about the existence of three main phases of global production, over the last 150 years, despite different theoretical explanations. In

at the centre of the analysis of the Monopoly Capital (MC) tradition (Baran and Sweezy, 1966), which carries out along the path traced by Hobson and his followers. Giant corporations are put again at center stage, identified as the fundamental engine of accumulation processes, macroeconomic dynamics, distributional as well as military conflicts (for a detailed review of the theory of MC see, among others, Foster, 2014; Sawyer, 2022). Governments, however, are no longer (or, at least, to a significantly lower extent) represented as 'internal forces', serving the process of accumulation and expansion of corporations as suggested by Lenin (1963 [1917]). The emphasis is rather placed on corporations' attempts to affect government actions (e.g., taxes and other redistributive measures, labor-protection laws, tariffs and limits on international expansion, etc.) that can foster/hinder their expansion (Cowling, 1982; Ietto-Gillies, 2012).⁴

With the advent of digital TNCs (digital platforms, hereafter) - e.g., paradigmatic examples are Amazon, Alphabet and Meta for the US, Alibaba and Tencent in the Chinese case (Rikap et al., 2021) -, relevant discontinuities are in order. The domination of a critical resource - i.e., information - that is essential to the very existence of capitalistic relationships, allows digital platforms to exert a degree of control vis-à-vis the economic space (labor, competitors, suppliers) going far beyond what MC' scholars documented concerning XX century's TNC (on this point, see Coveri et al., 2022; Pitelis, 2022; Vasudevan, 2022). And this reshapes the corporation-governments relationship too. To achieve their objectives, governments cannot do without the digital corporations' economic, technological and knowledge-related resources (Zuboff, 2019). Digital platforms, in turn, expand their reach (geo-

descriptive terms, we refer here to the three phases of globalisation: the first one starting after the first global crisis in the 1870s, the second one starting after WWII, the third one after the opening up of China to inward FDI and the collapse of the USSR (1980s-1990s). In theoretical terms, we consider them three different phases of the imperialism: either as colonial-non colonial-digital phases (Ietto-Gillies, 2021); or as national-multinational-TNC phases. Eventually, these might be named 'sub-stages', being imperialism the "highest historical stage of development" of capitalism (Lenin, 1963 [1917]).

⁴In this way, governments become, at least partly, 'external forces' to the corporation's growth and accumulation strategies. Therefore, the economic roots of nation states imperialistic strategies - including the operations of their security and military sectors - are (at least analytically) lost. In the literature, these are replaced by explanations that superordinate the sociological and/or political dimensions of conflicts, as done by Schumpeter (1972) in its 'Imperialism and social classes'.

graphically, sector and society-wise) at such a speed that contradictions and counter-reaction (e.g., foreign states trying to prevent digital platforms' access, workers' struggles, international movements and NGOs denouncing the incompatibility between digital corporations's activities and national regulations on privacy, taxation or labor rights) can hardly be coped without their government's help (Rolf and Schindler, 2023). In this respect, there is a fundamental discontinuity bringing some key elements of Hobson's and Lenin's Imperialism back to the fore. It is the *crasis* between today's dominant digital platforms and the security and military apparatuses of their home states. The latter are, at the same time, dependent on and participant to the development of those platform-dominated dual technologies (e.g., AI, cloud computing, IoT) that, on the one hand, are essential for competitiveness and growth in global markets and, on the other, vital for winning wars that are becoming increasingly digital (Gonzales, 2023).

Following up on a recent work (Coveri et al., 2022) and trying to bring together Imperialism (Hobson, 1902) and MC theories (Baran and Sweezy, 1966), in what follows we argue that digital corporations and governments are linked by a *mutual dependence* that, as in Lenin (1963 [1917])'s time, leads their respective strategies to influence and, in some cases, complement each other. We focus on the military sector as the latter is the domain where such dependence is more clearly expressed and where 'the economic roots of war' may become visible again (Pianta, 1989). To do so, we first analyze the evolution of state-corporation relationships, going from the early stages of Imperialism to the most recent developments of the MC theory (Section 2). Against this background, we delineate the key economic, technological and institutional drivers shaping the mutual dependence between digital platforms and military apparatuses (Section 3). Focusing on the US case, we then provide a quantitative-qualitative assessment of such dependence analyzing: public procurement (PP) contracts, defence-related infrastructures and technologies controlled by digital platforms as well as military-related activities (or activities directly instrumental to the pursuit of military objectives), in the context of the Russia-Ukraine war, in which such corporations are directly involved (Section 4). Finally, this evidence is discussed highlighting implications for economic theory, future research and policy (Section 5).

2. The imperialistic nature of war: yesterday and today

The starting point of Baran and Sweezy's most famous contribution (Baran and Sweezy, 1966, p.3-6) - 'Monopoly Capital: An Essay on the American Economic and Social Order' - is the recognition of the analytical shift from a competitive economy, as represented in the Marxian work⁵, to one dominated by monopolies and cartels, as in Lenin (1963 [1917])'s Imperialism (see the discussion above). In their words, Lenin 'gave full weight to the predominance of monopoly in the advanced capitalist countries. This was indeed a decisive advance in Marxian theory'. Baran and Sweezy (1966) identify the giant oligopolistic firm as the fundamental driver of surplus generation, as its continuously growing size goes hand in hand with the enlargement of the pool of exploited labor and, thus, of surplus to be accumulated. However, contradictions and limits to accumulation are always lurking, as in the case of insufficient purchasing power of wage earners, saturation of markets or competition from old and new global powers. And here comes the pressing need for corporations to 'internationalize' (i.e. export capital) via Foreign Direct Investments (FDIs) and to take advantage of the State (on this point, a fundamental contribution is that of Hymer, 1960).

According to Baran and Sweezy, governments play a key role in supporting capital reproduction and surplus accumulation.⁶ Even in this case contradictions are in order, though. The growth of public expenditures (e.g., welfare expenditures), find a limit in its distributive 'non-neutrality'. An excessive growth in public spending, particularly when the latter has to do with the provision of public goods relevant to the living conditions of wage earners, may very well translate into an increase in workers' bargaining power, undermining the foundations of accumulation itself. But this is where a peculiar sector of the public apparatus can come to the rescue of capital: the military sector. In the words of Baran and Sweezy (1966), 'the modern monopolistic systems have found a way out of permanent stagnation via defence [military] expenditure. Defence expenditure and wars are therefore seen as a way of

⁵It has to be highlighted that, among Marxists writing in the late XX century, this view of a Marxian analysis strictly focusing on competitive markets was not fully agreed. Indeed, the first book of *Das Kapital* (Marx, 2004 [1867]) implies explicitly only that commodities are always sold at their value.

 $^{^{6}}$ In their book, Baran and Sweezy (1966) provide a thorough empirical account of the growth of the US public expenditure vis-a-vis the consolidation of key oligopolistic corporations in both national and international markets.

bailing the capitalist system out of the tendency to permanent depression⁷⁷.

The analysis of Baran and Sweezy stops when the large oligopolistic enterprise evolves into TNC (Ietto-Gillies, 2012). Financialization, international fragmentation of production (i.e., outsourcing and offshoring), diffusion of ICTs: these developments allow TNCs to exert control and extract value well beyond their formal (physical and legal) perimeter, becoming an even more crucial (and complex) actor in determining the evolution of capitalism. Building on their contribution but going beyond Baran and Sweezy (1966)'s macroeconomic and 'under-consumptionist' perspective, Cowling (1982) includes micro (i.e., industrial organization) theoretical elements within the MC's edifice. In tune with this tradition, this author explores 'the division of national income between workers and capitalists in a world where monopoly or oligopoly capitalism dominates' and, paying tribute to Hymer (1960, 1970, 1972), focuses on how TNCs are able to 'coordinate production from one center of strategic decision-making when this coordination takes a firm across national boundaries'. Despite adopting a firm-level perspective, economic power is not seen, as in the neoclassical/mainstream definition, as mere 'market power', i.e., setting prices above the perfect-competition market clearing level. Rather, Cowling and Sugden (1998) defines TNCs' power as an external relation towards other economic and institutional actors, namely firms, suppliers, trade unions and governments. What TNCs plan 'inside' - geographical orientation, relationship with domestic and foreign rivals, governments and labour force - sets the 'rule of the game' outside. shaping accumulation and distributive patterns to their own advantage⁸.

The advent of digital platforms reshapes the nature of TNCs, including their relationship with markets and governments (Coveri et al., 2022) (Table 1 provides a synthetic account of the main discontinuities between 'traditional' TNCs and digital platforms). While XX Century's TNCs consolidate their presence at the times of managerial capitalism (Rahman and Thelen, 2019), digital platforms start rising when the 'neoliberal' paradigm is fully established (Mudge, 2008). Their growth takes place 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

⁷On this point, see the discussion in (Ietto-Gillies, 2021)

 $^{^{8}}$ A more detailed account of Cowling (1982) and Cowling and Sugden (1998)'s contributions is provided in Coveri et al. (2022)

state retrenchment, market liberalization, financial and trade globalization unfold at full steam, virtually everywhere. Differently from the TNCs studied by previous MC scholars' (see, among others, Ietto-Gillies, 2012), platforms are able to quickly expand their control (and associated value extraction) across countries, sectors and product segments relying on a relatively smaller amount of investments (both domestic and foreign), taking advantage of their 'lightness' (Ietto-Gillies, 2021) and of the close-to-0-marginal-cost reproducibility of the (digital) goods and services they produce (Coveri et al., 2022). The quasi-monopolistic control of information and related technology and infrastructures is remunerated by the market: the capitalization of large platforms grows relentlessly in spite of their relatively low profitability (Kenney and Zysman, 2020; Li and Qi, 2022). And this further accelerates their growth, providing additional resources to invest, selectively, in R&D and M&A activities that are crucial to maintain control (and technological primacy) in strategic fields such as cloud computing and AI (Fanti et al., 2022).

As the Internet becomes global, platforms expand their ability to control digital markets, critical infrastructure and services (both private and public) as well as the media where an increasing share of the public opinion is formed (and manipulated) (Culpepper and Thelen, 2020). And here the convergence between the expansionary strategy of platforms, aimed at monopolizing the digital market as well as the (dual) technologies on which it rests, and the imperialistic one of the State that gave birth to the Internet (i.e., the US), for which digital primacy means consolidation of economic and geopolitical hegemony, becomes more evident (Kwet, 2019). On the one hand, the retaliatory power of such new digital TNCs grows significantly with respect to their predecessors (Ietto-Gillies, 2021), as the peculiar domains under their control (e.g., social media) can determine whether political organizations and individuals are doomed to succeed or die^9 . On the other, the control of *dual* technologies, i.e. essential not only for the functioning of economic activities but also for homeland security and defense, transform platforms into governments 'eyes and hears', at home as well as abroad (see the next Section). More than 100 years after Hobson (1902)'s Imperialism, a peculiar state-

 $^{^{9}\}mathrm{A}$ 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

platform *crasis* seem to emerge, similar to the one bounding governments and oligopolistic cartels in the early XX century (Lenin, 1963 [1917]). Unravelling, again, the economic (and technological) roots of war. As US-based platforms techno-economic dominance increases in areas where their state's hegemonic capacity is strongest (Kwet, 2019; Franco et al., 2023), countermeasures are not long in coming: legal and technological barriers are erected (e.g., the Eruoepan Commission's GDPR), reactions multiply (e.g., the number of actions put in place by governments to curtail the power of platforms, such as by imposing hefty tax penalties or threatening to ban them from the country) and an hostile state-platform blocs is emerging, i.e. China (Rolf and Schindler, 2023). The latter raises the Great Firewall to limit the access of US-based platforms, while promoting the development of its national champions (e.g., Alibaba, Tencent) and strengthening its digital-military complex (Griffiths, 2021). In other words, the state-platforms mutual dependence represents a key feature of nowadays capitalistic conflicts as both the extraction of value as well as the production of the most sophisticated weapons comes through knowledge and technologies made possible by the fusion of their strategies. In the next section, we illustrate the main drivers laying behind such dependence, focusing on the domain where the latter is magnified: the military sector.

3. Mutual dependence and the digital platforms-military nexus

Governments are dependent on TNCs as the latter generate a substantial share of output and employment, 'complement' foreign policy through FDIs and internationalization strategies, hold assets and technological capabilities that are essential to govern change internally and exert hegemony externally (Arrighi, 1981). On the other hand, TNCs need governments to support their growth on foreign markets (e.g., trade agreements, diplomatic activities aimed at facilitating the penetration in specific markets), resolve internal (e.g., legal and security activities to contrast workers, trade unions or local organization' struggles, on this point see also Balcet and Ietto-Gillies (2020)) and external (e.g., settling disputes with foreign governments or corporations) conflicts, mitigate demand constraints through public expenditure and investment (Baran and Sweezy, 1966), support R&D projects characterized by radical uncertainty (Mazzucato, 2018). In the case of digital platforms, what the latter need most is to escape regulations aimed at reducing their market power (e.g., antitrust policies, forced sale/separation of business

	XX century's TC	Digital platforms	
Capitalistic phase	Managerial	Neoliberal	
Dominant sector	Manufacturing	Services	
Strategic objectives	Controlling the economic space by expanding physical assets and (to a lower extent) immaterial ones (e.g., patents, trademarks)	Controlling the economic space by expanding (selectively) physical assets and (extensively) immaterial (e.g., patents, trademarks) ones plus monopolizing data and data-related infrastructures	
Growth drivers	Supply-side economies of scale	Demand-side economies of scale: network effects, scope economies and lock-in effects	
Capital structure	Concentration and centralization	Centralization without concentration	
Corporate governance	High profits and dividend payout ratio, FDIs	Relatively low profits/revenues ratio, shareholder buyback, selective investments to control data-related infrastructures	
Internationalization strategies	Massive FDIs, directly exercised hierarchical control along SCs, centralization of R&D	FDI 'lightness', externalization and indirect control over formally independent economic actors, dominance over the innovation ecosystem	
Control over the labor force	Taylorism/Toyotism	Digital Taylorism	
Control over demand flows	Marketing and advertisment strategies	Targeted ads, 'anticipation' of demand flows, induced behavior	
Control over governments	Lobbying activity, retaliatory power (e.g., threat to offshore activities and employment)	Retaliatory power magnified by the control of data and strategic infrastructures (e.g., active role in military strategies)	

Figure 1: XX Century TNCs vs Digital platforms

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). As stronger the mutual dependence, as lower the risk for platforms to face regulations damaging their economic and technological dominance (Vasudevan, 2022). By the same token, platforms' systemic relevance further reinforce their position vis-à-vis governments, as the latter would hardly damage entities generating a substantial share of national income ¹⁰; and providing other firms with goods and services that are essential to their economic activity.¹¹

The military sector is where the state-corporation boundaries become more blurred (Pianta, 1989). First, the former is the domain where most of the radical innovations originate, to then be transferred to corporations standing to dominate the new technological paradigms (Dosi, 1982; O'Mara, 2020). Second, military-related public agencies are responsible for a large share of transformative R&D projects and innovative public procurement (PP)(Deleidi and Mazzucato, 2021), both essential tools for corporations to stick on the technological frontier. On the other hand, corporations are essential partners for the military sector since they have the idiosyncratic capabilities and organizational flexibility to develop incremental innovations and, thus, to preserve technological leadership. A role that is particularly critical when it comes to war-related digital technologies, as staying on the frontier means deter enemies and stay one step ahead in actual conflicts (Wong and Younossi, 2023). Moreover, their transnational nature makes platforms de facto outposts of their home state and, in particular, of military and security apparatuses. This is especially true when such corporations dominate foreign markets and/or are relevant (or exclusive) providers of critical goods and services to foreign governments. To some extent, these elements have characterized the relationship between the state and corporations well before the advent of platforms. As the latter step in, though, the same elements the same become an even stronger driver of strategic integration and mutual dependence.

¹⁰As of April 2023, the three major US-based digital corporations - i.e. Alphabet, Amazon and Meta - represented close to \$3 trillion in market value. Data retrieved from STATISTA, available at: https://www.statista.com/statistics/277483/market-valueof-the-largest-internet-companies-worldwide/. Last access 15 July 2023.

¹¹Large platforms provide vital services for companies operating in virtually all sectors, giving rise to what Cutolo and Kenney (2021) refer to as 'technological dependence'.

Originary linkage

To begin, an 'originary linkage' binding digital platforms and the military sector can be identified. During the XX and, even more so, the XXI's century, most of the breakthroughs giving rise to new industries and technological paradigms were linked to military programs (Polanyi, 2015). These are based on long-term investments, path-breaking R&D activities and 'missionoriented' 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 nations strategic autonomy (Edler et al., 2023) 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 (and/or already existing) corporations that from there on will reap the benefits of their 'first-mover' status (Mazzucato, 2018). To their advantage but, at the same time, increasing the geostrategic (and hegemonic) capacity of their nation state.

A large literature documents how military-related investments and R&D projects contributed to the emergence of new industries and firms (as well as promoting growth and upgrading of existing ones) (see, among others, Mowery, 2010; Jacobsen, 2015).¹² In this respect. 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 the major US Federal Agencies, in particular those related to the military apparatus as the DARPA (Mowery, 2010), contributed to the development of General-Purpose Technologies (GPTs), including semiconductors (Dosi, 1984) or the TCP/IP protocol (Greenstein, 2020), that have been crucial for the diffusion of personal computers and, later on, of the Internet itself (Mazzucato, 2018). In a nutshell, long-term activities carried out by its military apparatus and related R&D bodies are behind the substantial competitive advantage of the US in the nascent digital economy. Since the early days of the IBM's domination in the mainframe industry, US-based TNCs took the lion share of global ICT markets with some serious

¹²Likewise, the need to strengthen nation states' 'strategic capabilities' is always among the motivations explaining public efforts in areas, such as mining and infrastructure, that are not directly related to the military sector but that, in turn, may have a broader impact on nations' economic/technological sovereignty. This is testified by the direct involvement of security and military resources (and officials) in the development of such projects.

competition coming, starting only in the 1980s, from a bunch of Asian hightech companies (Japanese, above all others).¹³ In this context, the close relationships between DARPA, corporations and top universities, paradigmatic examples are Stanford and CalTech, favored technology transfer, 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, wherein military-related investments and R&D are of paramount importance, stands out. By the late-1990s, SV-based companies - i.e. nowadays' dominant platforms such as Amazon, Google and Facebook together with companies as Apple and Microsoft that, since the 1980s, were already playing a significant role in the computer hardware and software industry (O'Mara, 2020) - managed to catch the 'first train' to the newborn Internet economy, gaining dominant positions in critical market segments such as search engines (e.g., Google, now Alphabet), social networks (e.g., Facebook, now Meta), digital marketplaces (e.g., Amazon) and cloud services (e.g., Amazon Web Services, AWS).

Hence, US platforms dominating the Internet economy owe their emergence to the military apparatuses that supported the development of basic knowledge and technologies and, no less important, technology transfer (Mowery, 2010). Such 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 (e.g., the AI-related committees where, both in China and in the US, top military officials and platforms' CEOs share key technologies development strategies, see Lundvall and Rikap (2022)). The influence and control exerted

¹³Technological trajectories and related economic developments are never static processes, however. Since the early 2000s, China's industrial policy work tirelessly to narrow the technological gap vis-a-vis the US. And with remarkable results, as the former is challenging the US leadership in key technological domains as AI (Rikap et al., 2021) while the ongoing US-China 'Chip war' (Miller, 2022) testifies how intense the competition in this area has become.

by the military apparatus may become relatively less active and 'visible', as industries size and complexity increase and competition-driven incremental innovations dominate the evolutionary trajectory (Dosi, 1982). Nonetheless, formal (e.g., laws and regulations) and informal (e.g., moral suasion) instruments aimed at influencing corporations' strategies and, more importantly, preventing the latter to clash with security, foreign policy and military agendas, are always in order (Lundvall and Rikap, 2022). On the other hand, the active role of military-related institutions can return to the forefront, as is happening at this stage with AI or quantum technologies (Gonzales, 2023), at a time when resources and strategic direction are needed to push forward the technological frontier, especially when it comes to dual technologies with relevant security implications. As technological and geo-strategic conditions require it, the original linkage is revitalized and, with it, the integration of state-corporation strategies.

Knowledge, technology and critical infrastructures

Today's wars are, to a large extent, digital (DoD, 2023). The most advanced weapons (e.g., drones, missiles, aircrafts) and defense systems (e.g., anti-aircraft systems, radars) are based on technologies such as AI (Johnson, 2019) or new-generation satellites (e.g., low Earth orbit (LEO) satellites, as the ones produced by the Elon Musk' Space-X). Cyber-attacks (e.g., hostile actions aimed at damaging the enemy's communication system, stealing critical information and or disrupting vital infrastructures) and actions aimed at preventing them are becoming a matter of life or death during a war. Likewise, digital technologies are needed to pursue security and intelligence activities (Brayne, 2020), both at home and abroad. Therefore, being on the (digital) technological frontier and, hence, preventing enemies to get close to it is a fundamental objective for governments and their military apparatuses Rolf and Schindler (2023). As largely documented, such frontier is dominated by few global (US and Chinese) platforms (see, among others, Coveri et al., 2022; Kemmerling and Trampusch, 2022). The latter monopolize key technological assets (i.e., servers, cloud infrastructures, submarines cables) (Gjesvik, 2023), hold the majoritarian share of digital patents (Fanti et al., 2022; Maslej et al., 2023) and are the locus where most of the formal and tacit knowledge, essential to move forward along technological trajectories (Dosi, 1982), is developed (Rikap et al., 2021).

In this context, mutual dependence is explained by both 'material', formal as well as 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. Exclusivity and robustness of such control are related to the very nature of digital technologies, characterized by cumulativeness, economies of scale and network effects (Ietto-Gillies and Trentini, 2023). As a critical digital infrastructure (e.g., cloud servers) grows in terms of size and relevance, e.g., increasing the mass of information stored and processed, the efficiency of related technologies (e.g., ML algorithms) and the uniqueness (and 'black-boxishness') of corporationspecific competences increase too. This may strengthen platforms' position vis-a-vis both potential competitors as well as governments (Coveri et al., 2022). Consider a government facing the need to set up a new surveillance system, access sensitive information, respond to (or perpetrate) a cyberattack, or deploy a satellite system in a given area: these goals can hardly be achieved in a reasonable time span without partnering with one of the platforms controlling relevant knowledge and technological assets. Mutual dependence is further reinforced by the pivotal role that key digital corporations play in both civil and military innovation ecosystems (Rikap et al., 2021; Gawer, 2022). By governing knowledge co-creation processes and exploiting the modular structure of digital ecosystems platforms are able to benefit from the decentralized nature of digital innovation while preserving their power, both economic and technological. And the same dynamics apply to militaryrelated supply chains and innovation ecosystems. 'Traditional suppliers' of the military apparatus (e.g., major suppliers of armaments and equipment for military forces such as, in the US case, RTX or Halliburton) cannot do without the technologies, components and related services provided (often under monopoly conditions) by the platforms and, without which, digitization of armaments is hardly achievable (Wong and Younossi, 2023). Another related driver of dependence concerns competences and training activities. In high-tech industries and, in particular, in the digital domain, competences tend to be complex, idiosyncratic, technology and organization-specific. As a result, recruiting 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, other firms and public bodies. This is due to the career prospects the former can offer and incomparable economic levers (e.g., stellar salaries and stock options) they can rely on (Rikap, 2023). As a result, governments (and other firms) may face a substantial dependence on key digital platforms, particularly when it comes to the introduction of new technological

solutions and related training activities, as the latter tend to monopolize the skills needed to pursue such activities. No less relevant, sector-specific managerial competences 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, brought about by the fact that major geopolitical players are investing to excel in digital warfare, their home states (i.e. China and the US) have no choice but to involve platforms' top managers in key technology development projects. As documented by Lundvall and Rikap (2022), their role is formalized in various bodies of public importance, linked to the military agencies, aimed at developing frontier technologies (e.g., AI).

Digital platforms as 'eyes and ears' of governments

Since the early days of the *East India Company*, the intermingling of the economic interests of TNCs, on the one hand, with diplomatic, intelligence and military activities of nation-states, on the other, is commonplace (Hobson, 1902). The overseas presence of corporations provides a unique tool for seizing sensitive information and managing relationships with local government and elites so as to increase ramification and effectiveness of geopolitical strategies. Military and intelligence apparatuses, in turn, are often key partners of domestic corporations looking for foreign expansion: protecting assets and personnel, ensuring the security of logistics, and providing support in case of conflicts with local authorities and organizations. Here, the 'integration' of corporations' expansionary strategies and nation-states (foreign) intelligence and geopolitical objectives may represent another key driver of mutual dependence.

Instability 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 - i.e., companies that given their economic exposure in a given country forge close relationships with the local government despite tensions that may exist between the latter and the home country one. The latter, in turn, are subject to sudden shocks and shifts, which tend to be ill-matched with the fixed costs and long-term investments required to penetrate foreign markets. In this respect, worsening (or, even more so, compromising) relationships with a given foreign country can be a dry, even capital, loss for the most exposed corporations (Rolf and Schindler, 2023). Their reaction, in this case, may be to try conditioning the government - relying on lobbying (Culpepper, 2010), retaliatory power (Ietto-Gillies, 2012) or other means (Culpepper and Thelen, 2020) - so to avert the disruption of relevant economic interests.

Concerning digital platforms, the degree of strategic integration and, hence, of mutual dependence may increase substantially. The main USbased platforms (e.g., Alphabet, Amazon, Microsoft, Facebook) control a large share of the digital information circulating globally. Due to the competitive advantage they have accumulated since the early stages of the Internet (see above), the technological primacy they have in terms of digital patents (Hötte et al., 2023) and dominance in their innovation ecosystem (Rikap et al., 2021; Gawer, 2022), these corporations monopolize services that are crucial both in the civil sphere, for the production of public goods as well as for security and military purposes (O'Mara, 2020). This makes them essential partners for businesses and public authorities alike, both at home and abroad. At home, platforms are a fundamental 'arm' of their government's security, intelligence and law enforcement activities. Focusing on the US case, Goodwin (2018) reports that, between January and June 2017, Facebook received 32.716 requests for information from U.S. law enforcement, including requests on 52.280 user accounts, 19.393 search warrants and 7632 subpoenas. Similarly, Alphabet received 16.823 requests regarding 33.709 accounts while Twitter 2.111 requests concerning 4594 accounts. Platforms have produced at least some information for about eighty percent of requests. Goodwin (2018) underlines that platforms operate as "surveillance intermediaries holding extraordinary power". Such power is related to their large degree of discretion when processing government requests: "discretion in how critically they evaluate the legality of requests, in slowing down the process by insisting on proceduralism, and in minimizing their capacity to respond to legal requests by implementing encryption. This discretion means that surveillance intermediaries determine, at least in part, the government's access to information about our personal relationships, professional engagements, travel patterns, financial circumstances, and much more."

Abroad, platforms become 'eyes and ears' of their home state intelligence and military apparatuses, as the former can access sensitive information while it is arduous for foreign governments and companies to know what happens to that same information once absorbed by platform-dominated infrastructures. The limits to such a techno-infrastructural dependence, if any, are geopolitical. To avoid subjugation to US corporations (and, thus, to the partially integrated US intelligence and military apparatuses), countries such as China, Russia, or Iran have banned the former from accessing their domestic market while creating own networks and supporting the growth of national platforms (e.g., the Chinese Alibaba, Tencent or JD) (Li and Qi, 2022). This strategy allowed China to develop its own platform ecosystem which, as in the US, is substantially integrated with the state and its civil and military apparatuses (Lundvall and Rikap, 2022; Rolf and Schindler, 2023). More broadly, by partnering with corporations that control critical technologies and infrastructures - such as, for example, cloud (Rikap and Lundvall, 2022), AI(Fanti et al., 2022), blockchain (Beaumier and Kalomeni, 2022), 5G technologies (Wu, 2020) and undersea cables (Gjesvik, 2023) - nation states (i.e., China and the US) can strengthen their grip on economies included in their 'sphere of influence', gain advantage over enemies or enact what (Kwet, 2019, p. 4) 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 (similar dynamics may be envisaged in China too, see Rolf and Schindler (2023)). Such a 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 [italics added] in the international community. Assimilation into the tech products, models, and ideologies of foreign powers – led by the United States – constitutes a twenty-first century form of colonisation." In other words, being the exclusive suppliers of services for both business growth as well as for the strengthening of key public services, such as education and health, digital corporations become the 'tool' for ensuring economic and geopolitical subordination, particularly where digital penetration occurs in a totalizing and pervasive manner (as in developing countries lacking substantial infrastructures, technologies and competences). A similar dynamic to the one documented by Kwet (2019), who focuses on the South African case, can be observed in Southeast Asia and in economies that are coming into China's sphere of influence. In this regard, the alliance is between the Beijing government, its security/military apparatuses and China-based platforms, such as Alibaba or Tencent (Keane and Yu, 2019).

4. The digital platforms-military nexus: an empirical assessment

In what follows, we provide a quantitative and qualitative assessment of the digital platforms-military nexus. The focus is on the US case, as this is where the originary linkage has been established (see above) and, no less relevant, most of the dominant platforms are based. Moreover, the integration between the US military apparatuses and digital platforms is likely to be magnified by the current confrontation with China. A confrontation that is largely played on technology, shaped by the US attempt to limit the Chinese economic and technological catching-up (Rikap et al., 2021). On the other hand, China is the home of the largest non-US digital platforms having a global scale - e.g., Alibaba, ByteDance, Tencent - and represents the most powerful challenger to the US technological (and, hence, military) supremacy (UNCTAD, 2019; Hötte et al., 2023). Focusing on such a growing competition, Rolf and Schindler (2023) have recently shown how both the US and Chinese governments *leverage their domestic platforms to secure the control of data and extend their economic and military projection overseas*.

First, we analyze the evolution of the US Department of Defense (DoD) procurement contracts, showing the growing relevance of platforms as DoD procurers. As a complement, we systematically review official documents and relevant technical reports (e.g., Wong and Younossi, 2023) to show the growing importance of digital technologies for the DoD's R&D and procurement plans. 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 militaryrelated objectives (Shull et al., 2020) but are also characterized by high complexity, cumulativeness, and strong complementarity with their idiosyncratic capabilities (Mowery, 2010). In doing so, we document the pivotal role played by platforms as promoters and coordinators of innovation ecosystems wherein digital start-ups are nurtured to develop technologies of military relevance (Gawer, 2022). This makes it possible to evaluate the degree of dependence between Federal agencies (e.g., DoD, CIA, NSA) entrusting platforms with the management of critical services, on the one hand; and platforms, monopolizing the underlying technologies and knowledge, on the other. Third, we analyze the available evidence on the active participation of key USbased platforms (i.e. AWS, Meta, Microsoft) into the Russia-Ukraine war, highlighting a fundamental discontinuity concerning the relationship between military apparatuses and private corporations. Unlike traditional procurers,

platforms do not simply provide critical assets/services to security and military agencies but manage such services directly and, often, in a context of unprecedented intermingling with the civilian sphere (e.g., cloud infrastructures). From the perspective of platforms, this means, on top of controlling the accumulation of production and technological capabilities, contributing to develop 'relational skills' and access sensitive information in critical 'national security' situations. Two elements that can significantly strengthen the platforms-military mutual dependence.

DoD procurement goes digital

To contextualize the analysis, we first of all document the structural relevance of military-related R&D in the US. Figure 1 reports the government budget allocations for R&D (GBARD) for Defence, focusing on the US and a set of selected western economies (from 1995 to 2021). The figure shows that the share (%) of GBARD for defense over total GBARD for the US is much higher over the whole period than for all the other countries considered (France, Germany, Japan, South Korea and Japan), with the former hovering around 55% in the second half of the 1990s and fluctuating around 45% in the first two decades of the 2000s. Interestingly, the gap between the US and the other economies considered has widened over time: data for the latter countries show figures ranging from less than 40% in the second half of the 1990s to less than 20% since 2010. All in all, the US technological leadership is confirmed to be fundamentally intertwined with continuous R&D efforts put forht by its military apparatus (Mowery, 2009, 2010).

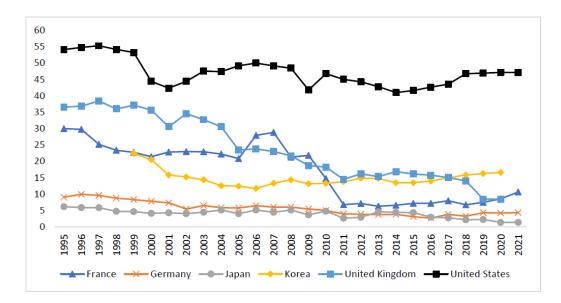


Figure 2: GBARD for Defence (% of total GBARD), selected countries, 1995-2021 Source: OECD

According to the 'US DoD 2024 budget request' DoD (2023), the Fiscal Year (FY) 2024 acquisition (Public Procurement (PP) and Research, Development, Test, and Evaluation (RDT&E)) funding is going to reach \$315.0 billion, which includes funding totaling \$170.0 billion for PP and \$145.0 billion for RDT&E. For the budget mission 'Command, Control, Communications, Computers, and Intelligence (C4I) Systems' the 'Office of the Undersecretary' requests \$14.5 billion, about the 5% of the total DoD investment budget. Albeit it may seem a rather small percentage, it should be noticed that digital components are now crucial to develop virtually all the all armaments included in the DoD budget. Concerning the C4I, digital goods and services are needed to perform a number of key military activities: "command centers: communications gear: air traffic control: night vision equipment; cyberspace activities (cybersecurity, cyberspace operations, and supporting $R \mathcal{E}D$; data processing equipment; fire control systems; other information technology; and related systems...a large number of programs such as Tactical Network Transport (TNT), Handheld Manpack Small Form Fit (HMS) radio, Joint Regional Security Stacks (JRSS), Information Systems Security Program (ISSP), Crypto devices and key management infrastructure, Nuclear Command and Control, equipping the Cyber Mission Forces, the Air Force National Airborne Operations Center (NAOC) Recapitalization program, the Navy's Consolidated Afloat Networks and Enterprise Services (CANES), and the Integrated Personnel and Pay System-Army (IPPS-A). Remarkably enough, the (DoD, 2023, p.8) states that "the FY 2024 funding is substantially higher than the amount requested in FY 2023, primarily because of increased funding for Cyberspace, Spectrum, AI, 5G, and other emerging technologies." Overall, DoD budget requests related to the C4I mission almost doubled between 2017 and 2023, moving from 7.4 to 12.8 billion \$. An even more pronounced upward trend - from 7.1 in 2017 to 21.7 billions in 2023 - regards the 'Space Based System' mission, including a number of technologies and applications with respect to which platforms play an important role as, for example, in the case of SpaceX (or are planning substantial investments in that direction, as in the case of Amazon). Finally, the FY2024 funding request for 'Science and Technology' (S&T) "represents the highest funding for advance research in the history of the DoD (DoD, 2023, p. 14). Key technologies include: AI, ML applications, Hypersonics (offensive and defensive), Directed Energy (lasers, particle beams, etc.), Microelectronics, Biological Technology, Cyber, Fifth Generation communications (5G), Autonomy, Space, and Quantum sciences. These are identified by the DoD as "vital cutting-edge capabilities to the warfighter...needed to protect the United States, its allies, and American forces worldwide".

We now dig into the official source of US public procurement data – USAspending.gov – shedding light on the growing reliance of the US military apparatuses on technologies developed by digital platforms. Figure 2 shows the number of Alphabet (Google), Amazon, Facebook and Microsoft's contracts stipulated with US federal agencies (including the DoD) over the period 2008-2022. These figures highlight that a major acceleration in the total number of contracts awarded to digital corporations occurred since the beginning of the considered time span. From 2009 to 2018, digital platforms have been awarded with more than 200 contracts per year, while a decreasing trend is observed since 2019. The figure also shows that the lion's share of contracts was awarded to Microsoft and, to a lower 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.

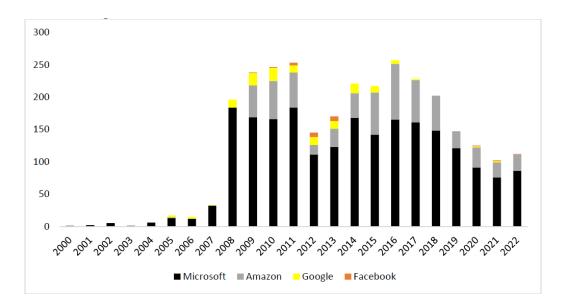
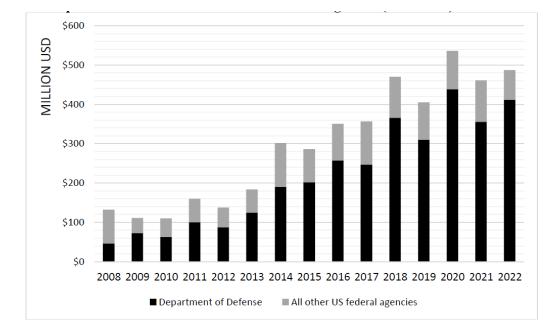


Figure 3: Number of Amazon, Google, Facebook and Microsoft's contracts with all US federal agencies, 2000-2022 Source: USAspending.gov

Figure 3 reports the overall value of contracts awarded to digital platforms in monetary terms, distinguishing between those stipulated with the DoD and other US federal agencies. Overall, the figure shows that the monetary value of military (and security) procurement contracts has grown rather steadily from 2008 to 2021. Microsoft reports by far the greater value of both contracts with DoD and other US federal agencies: more than 4.4 USD billion over the whole period, of which about 3.2 billion awarded by the DoD. This means that about 75% of the value of all contracts stipulated by US agencies with Microsoft have been awarded by the DoD. Amazon follows at a distance: the value of contracts for this corporation is about 128 million over the whole period, of which about 50 million awarded by the DoD (equal to little less than 40% of the value of all contracts awarded to Amazon by US federal agencies)¹⁴ Consistently with Figure 2, we find that the value of

¹⁴If one includes the value of subcontracts, i.e., contracts awarded by US federal agencies to recipients that subcontracted part of the service to a platform, the situation does not change much. The value of the overall subcontracts awarded to Microsoft by all US federal agencies is equal to 1.7 billion over the whole period, of which about 1.4 USD billion (indirectly) awarded by the DoD (82% of the overall value of subcontracts). As for



the contracts awarded to Alphabet and Facebook is relatively small (Maaser and Verlaan, 2022).

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). Nonetheless, there are good reasons to believe that these data underestimate the role of platforms as relevant suppliers of the

Figure 4: Total value of Amazon, Google, Facebook and Microsoft's contracts with the Department of Defense and other US federal agencies (2008-2022) Source: USAspending.gov

Amazon, the value of the overall subcontracts awarded to this platform by all US federal agencies is equal to about 450 million over the whole period, of which slightly more than 200 million (indirectly awarded) by the DoD (45% of the overall value of subcontracts).

military apparatus (for a thorough investigation, see Maaser and Verlaan, 2022; Gonzales, 2023). In fact, USAspenging data do not include major contracts, 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 which are not included in the official US spending database; as well as to the multi-year nature of such large awards, whose accounting allocation might make them less detectable (Paulson, 2021, 2022).

Building on a number of different sources (e.g., technical reports, companies documents/websites and journal articles), we now provide a systematic illustration of recent multi-year federal contracts entrusting platforms to develop (manage) key technologies and infrastructures. In early 2013, the Central Intelligence Agency (CIA) awarded a contract to Amazon Web Services (AWS) worth up to \$600 million over a period of 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.¹⁵ In 2014, AWS launched its first "Top Secret Region", called "Top Secret-East", designed to host the US government's top secret classified information.

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

Year and Department/Agency	Contractor	Value (\$)	Nature of service	Declared aim
2013 – CIA	Amazon	600 million	Cloud	Data management aimed at preventing terrorist attacks
2019 – DoD	Amazon and Microsoft	50 million	Drones	Defence
2020 – CIA	Alphabet, Amazon, Microsoft and Oracle	"Tens of billions" ¹⁶	Cloud	"Commercial Cloud Enterprise" (C2E) project – cloud services centralized for 17 intelligence agencies
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 ("WildandStormy" project)
2022 – DoD	Amazon	NA	Start-up accelerator	Coordination of cloud- based activities and promotion of start-ups of military relevance
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)

Figure 5: Selection of multi-year military and security contracts signed by main US digital platforms

Source: Amazon official website, CNBC, Forbes, New York Times

In 2017, this was followed by the launch of a second 'Top Secret Region', called 'Top Secret-West', providing additional cloud capacity for US intelli-

gence and defense agencies, including the CIA and NSA.¹⁶ Such services are part 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 in order "to save time and resources for warfighters and analysts".¹⁷ As reported by the AWS 'Public Sector Blog', Battlefields across land, air, sea, and space are increasing in weapons lethality, and the speed and accuracy with which military forces need to securely detect and engage enemy targets is exponentially increasing. AWS capabilities can $[\ldots]$ automate and scale manual sensor-to-shooter processes so that teams can focus on mission-critical tasks. And, use advanced analytics and AI and ML-enabled capabilities to increase shooter accuracy, particularly for targets beyond the *line of sight.* Notably, similar cloud infrastructures for US national security missions, specifically aimed to speed up the delivery of defense and security workloads classified as "top secret", have been launched also by Microsoft, i.e., the "Azure Government Top Secret" in 2021 followed by the "Azure Government Secret" in 2017.¹⁸ In November 2020, the CIA confirmed the award of its "Commercial Cloud Enterprise" (C2E) contract to roll out new cloud hosting capabilities for the 17 federal intelligence agencies. AWS, Alphabet, IBM, Microsoft and Oracle will compete for specific task orders over the next 15 years under a contract that could be worth "tens of billions" of dollars.¹⁹

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. Remarkably, this contract follows a \$480 million contract Microsoft received to give the Army

Last access: Last access: July 15 2023. ¹⁷See https://aws.amazon.com/federal/us-intelligence-community/ Last access: July 15 2023.

¹⁸See 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.

¹⁹See https://gcn.com/cloud-infrastructure/2020/11/cia-awards-massive-cloud-contract/315771/. Last access: July 15 2023.

prototypes of the Integrated Visual Augmented System (IVAS) in 2018.²⁰

In September 2021, Amazon and Microsoft picked up \$50m in US military drone surveillance contracts, following Alphabet dropping Project Maven. The latter is a DoD AI programme designed to process full-motion images and video from drones in order to automatically detect potential targets. In 2018, more than 3.000 Alphabet employees signed a petition expressing concern about the military use of AI, asking the company to abandon the project.²¹ Following this protest, Alphabet effectively abandoned the Maven project in early 2019²², being replaced by Microsoft, starting a \$30 million contract in 2019, and AWS, winning a \$20 million in 2020.²³

In April 2022, the NSA awarded a \$10 billion cloud computing contract to AWS. This contract, called 'Wild and Stormy' (WaS) is a cloud computing services contract in support of the NSA's 'Hybrid Compute Initiative' (HCI), aimed at addressing the NSA's significant and delicate processing and analytical requirements. AWS is now the HCI cloud provider managing the process of moving the NSA's global intelligence and surveillance data from internal servers to the cloud.²⁴ In May 2022, AWS has selected 10 startup participants for its first Defence Accelerator programme for UK-based startups. AWS worked with the UK government technology consultancy 'Public'

²⁰See https://www.cnbc.com/2021/03/31/microsoft-wins-contract-to-make-modifiedhololens-for-us-army.html. In addition, in June 2021 "the Department of Defense has awarded Dell a \$2.5B blanket purchasing agreement to provide the U.S. Navy with enterprise software licenses. Under terms of the five-year deal, the technology company will provide user-based subscription licenses for products including Microsoft 365 and Microsoft Azure. The contract award comes as the DOD transitions to DOD365, which is a higher-security version of Office365 that was purchased through the \$4.4 billion Defense Enterprise Office Solutions (DEOS) contract." (source: https://fedscoop.com/2-5-billiondollar-contract-dell-enterprise-software/).

²¹On this point, see: https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html)

 $^{^{22}}$ See: https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html)

²⁴Remarkably enough, the WaS contract was once a classified secret and become of public knowledge due to the legal dispute that existed between Microsoft, which disputed 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

to select the accelerator's participants. The main goal of the programme is to foster military and defence-related technological capabilities of startups, such as cyber defence solutions, data discovery and optimisation, and space exploitation, by means of cloud technologies. In August 2022, the US Army integrated the breakthrough technology designed by Microsoft into Stryker armored vehicles that offer the capabilities Soldiers need to regain and maintain overmatch in multi-domain operations on battlefields. In June 2022, Alphabet announced the creation of 'Google Public Sector' (GPS), a new division aimed at helping US public sector entities in accelerating their digital transformations. Few months later, GPS announced the provision of the Google's workspace to 250.000 personnel of the U.S. Army. Finally, in December 2022, Alphabet, Amazon, Microsoft and Oracle have been awarded a 9 billion DoD contract to set the Joint Warfighting Cloud Capability (JWCC) by the DoD.²⁵ This project is designed to allow the DoD to fully leverage the capabilities of the cloud for military and defense-related activities, in order to foster "the nation's ability to stay a step ahead of adversaries."²⁶

This evidence displays the growing importance of digital platforms as Federal agencies - including the DoD (DoD, 2023) - providers of key technologies related to security and defence (Maaser and Verlaan, 2022; Gonzales, 2023). And this certifies one side of the mutual dependence: governments (and, more specifically, their security and military apparatuses) are dependent on the skills and technologies of a small group of platforms to perform essential functions (e.g., managing sensitive information). On the other hand, the resources provided by the DoD and other Federal agencies are of increasing importance for platforms, both in monetary terms and as demand-pull innovation drivers (Mowery, 2010). This is testified by the fact that making weapons (and/or their digital components/counterparts) is becoming one of their most strategic activities (Gonzales, 2023). As argued above, this can be also related to the participation of platforms' top representatives in public institutions aimed at developing and controlling military-related technologies. A paradigmatic example is that of Eric Schmidt, former Alphabet's CEO. Together with former Secretary of State Henry Kissinger and ex-Deputy of

 $^{^{25}\}mathrm{See:}$ https://edition.cnn.com/2022/12/08/tech/pentagon-cloud-contract-big-tech/index.html

²⁶For a description, see: https://aws.amazon.com/blogs/publicsector/aws-selected-for-u-s-department-of-defense-joint-warfighting-cloud-capability-contract/.

Defense Secretary Robert Work²⁷, Schmidt was member of two government advisory boards – namely, the Defense Innovation Advisory Board and the National Security Commission on AI – aimed at jump starting technological innovation at the DoD in order to counter the emerging technological power of China. At the same time, Schmidt relied on his own venture capital to invest into more than six defence start-ups, thus becoming a relevant actor on 'both sides of the table'.²⁸

Digital platforms go to war

An even stronger evidence of the linkages between platforms and the military apparatus regards their active participation into warfare activities. This is the case of the war in Ukraine, where key US-based platforms have, since its very early stages, taken an active role concerning the deployment of critical information-related infrastructures and technologies (Coveri et al., 2023). The archetype is Space-X, 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. ²⁹ The Starlink terminals have been 'donated' (or purchased by the US government) by Space-X to "help Ukrainian troops operate drones, receive vital intelligence updates and communicate with each other in areas where there are no other secure networks." ³⁰

Notably, in September 2022 the sudden shutdown of Starlink almost jeopardised a decisive military operation carried out in the eastern part of Ukraine. Shortly after these events, Elon Musk, Space-X's owner, finalized the acquisition of another key digital corporation – i.e., Twitter – and engaged in a negotiation with the US government (as well as with his European

²⁷As Deputy Secretary of Defense, in office from 2014 to mid-2017, Robert Work was also the major proponent and advocate of the so-called "Third Offset", namely the competitive strategy aimed to leverage U.S. advanced technologies to offset China's and Russia's technological advances (Gentile et al., 2021).

 $^{^{28}\}mathrm{See}$ https://www.nytimes.com/2020/05/02/technology/eric-schmidt-pentagon-google.html

²⁹See Srivastava, M., Olearchyk, R., Schwartz, F., & Miller, C. "Ukrainian forces report Starlink outages during push against Russia", Financial Times, 8 October 2022. Last access: 8 October 2022.

³⁰See https://visitukraine.today/blog/1046/starlink-why-the-internet-from-elon-musk-is-crucial-for-ukraine; see also https://www.ft.com/content/9a7b922b-2435-4ac7-acdb-0ec9a6dc8397

allies) regarding the financing of Starlink. A month later, Musk has been reported (although he denied it) to hold a direct channel with Putin discussing his own 'peace plan' for Ukraine.³¹ Two elements stands out here. First, the crucial role played by a private corporation, whose activity is theoretically intended for the civil sphere, into a war, something that is likely to significantly increase its bargaining power vis-a-vis the government. Second, the military apparatus' heavy reliance on Space-X technologies to pursuit key battlefield objectives. Among other things, the latter may help explaining the overall malleability of the US government vis-a-vis Musk's strategies including those, such as the acquisition of Twitter, capable of intensifying the mutual dependence.

Space-X is not alone in playing an active role in the Ukraine war, tough. First all, virtually all US-based platforms cut their services in Russia and Belarus as soon as the war started. Even more relevant, AWS disclosed that, as early as February 24 2022, its technical staff was "on the ground in Ukraine to ensure the fastest transition of all relevant data (e.g., government, banks) to the AWS Cloud". 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 has stated that when the war is over, there will be no reason to go back anyway. Since 6 October 2022, Amazon has removed referral fees for Ukrainian SMEs selling their products on its European marketplace. And the same goes for Microsoft. The latter has just committed to provide \$100 million worth technology "to ensure that government agencies, critical infrastructure and other sectors in Ukraine can continue to serve citizens through the Microsoft Cloud". Apple also 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 have blocked Russian state media channels RT and Sputnik from the Youtube platform, while Facebook (Meta) opted for excluding from Facebook and Instagram contents stemming from media that are close to the Kremlin.

Overall, platforms' active participation into warfare activities is another element that may help explaining mutual dependence. As platforms become vital partners to pursue a large number of military activities, the DoD can

³¹See https://fortune.com/2022/10/11/elon-musk-ian-bremmer-putin-russia-ukraine/

do nothing but seek stable and effective partnerships with them. In this respect, the bargaining power of platforms may grow as the amount of critical information under their control and the exclusivity of the technology-specific capabilities they develop increase too. On the other hand, being involved in close relationships with state ganglias (i.e., the military) operating with a hierarchical logic that is far away from the flexibility characterizing market relationships, exposes to risks and may reduce platforms' strategic/operational flexibility Pianta (1989). No less relevant, the integration between platforms and the military apparatus could be threatened by the conflict between top managers, aimed at meeting DoD's demand, and high skilled personnel- e.g., engineers, software developers - which may consider the development of warrelated technologies ethically unacceptable (Gonzales, 2023).

5. Discussion

The state-market-corporation boundaries are at the center of socio-economic analyses at least since Marx (2004 [1867]). Hobson (1902) and Lenin (1963 [1917]) have recognized the convergence of the interests (and strategies) of the state, on the one hand, and monopoly capital, on the other, as the main engine of capitalist evolution as well as the cause its main contradictions, including military conflicts. In this paper, we have built on MC theories (among others, Baran and Sweezy, 1966) showing how digital platforms represent a discontinuity in the state-corporations relationship, 'blurring' its boundaries and giving rise to a form of 'mutual dependence'. In addition to their systemic relevance, which allows platforms to activate effective 'retaliatory power' vis-a-vis public authorities (Ietto-Gillies, 2012), such dependence is fundamentally related to the complex, cumulative and idiosyncratic nature of the productive and technological capabilities characterizing such corporations. This is particularly true in the security and military sector, where technological dependence is strong and the state-platforms overlap turns out to be substantial. On the other hand, the resources and support that the state provides to platforms is of utmost importance as an accumulation mean, demand-pull innovation driver as well as a tool to break down barriers to domestic and foreign expansion. Three major elements help explaining the state-digital platforms mutual dependence: 'originary linkage'. critical nature of infrastructures and technology controlled by platforms and their role as their government's 'eyes and ears' (both at home and abroad).

Building on quantitative and qualitative data and focusing on the US case,

we have documented the increasing relevance of platforms as DoD procurers. No less relevantly, their role as masters of almost all key strategic informationrelated infrastructures is emerged. Finally, digital platforms seem to differ from more traditional TNCs insofar they are not only critical suppliers of the military apparatus. Remarkably enough, such corporations develop and deploy the same dual technologies that enable them to dominate the digital market playing an active role in war scenarios, such as the current Ukraine war. Obviously, the relationship between the state and corporations (including platforms) is much more complex than what has been conveyed here. Therefore, further research is necessary. In this respect, three elements are worth mentioning. Although we emphasized the convergence between corporate and state strategies, the latter can easily clash to the extent that, for example, the expansion of the former leads to actions contradicting the objectives of the latter (and vice versa). Additionally, we have not taken into account the fragmented and conflictual nature of public powers, including the political dimension. The state and its apparatuses are not monolithic; interest groups in perpetual conflict shape their forms and orientation, including their relationships with corporations. This can have significant effects on the degree of mutual dependence. Likewise, strong dependence can influence the forms and evolution of institutions.

Finally, this work sheds a sinister light on digital technologies often naively considered as 'neutral' and capable of indiscriminately improving human condition. On the contrary, if their development is constrained between defending monopolistic interests and designing technologies capable to effectively surveil and kill, there seem to be grounds for a brand new 'Luddism'. This time driven not (or not solely) by the fear of mass unemployment. But by a more general desire to preserve the human race from the perverse alliance of public and private (assuming that this distinction makes any sense) sorcerer's apprentices.

References

- Arrighi, G., 1981. The geometry of imperialism: The limits of hobson's paradigm. Science and Society 45.
- Balcet, G., Ietto-Gillies, G., 2020. Internationalisation, outsourcing and labour fragmentation: the case of fiat. Cambridge Journal of Economics 44, 105–128.

- Baran, P.A., Sweezy, P.M., 1966. Monopoly Capital. An Essay on the American Economic and Social Order. Monthly Review press Press.
- Beaumier, G., Kalomeni, K., 2022. Ruling through technology: politicizing blockchain services. Review of International Political Economy 29, 2135– 2158.
- Brayne, S., 2020. Predict and Surveil: Data, discretion, and the future of policing. Oxford University Press, USA.
- Coveri, A., Cozza, C., Guarascio, D., 2022. Monopoly capital in the time of digital platforms: a radical approach to the amazon case. Cambridge Journal of Economics 46, 1341–1367.
- Coveri, A., Cozza, C., Guarascio, D., 2023. War in the time of digital platforms. Social Europe, Available at: https://www.socialeurope.eu/war-inthe-time-of-digital-platforms.
- Cowling, K., 1982. Monopoly capitalism. Macmillan International Higher Education.
- Cowling, K., Sugden, R., 1998. The essence of the modern corporation: markets, strategic decision-making and the theory of the firm. The Manchester School 66, 59–86.
- Culpepper, P.D., 2010. Quiet politics and business power: Corporate control in Europe and Japan. Cambridge University Press.
- Culpepper, P.D., Thelen, K., 2020. Are we all amazon primed? consumers and the politics of platform power. Comparative Political Studies 53, 288– 318.
- Cutolo, D., Kenney, M., 2021. Platform-dependent entrepreneurs: Power asymmetries, risks, and strategies in the platform economy. Academy of Management Perspectives 35, 584–605.
- Deleidi, M., Mazzucato, M., 2021. Directed innovation policies and the supermultiplier: An empirical assessment of mission-oriented policies in the us economy. Research Policy 50, 104151.
- DoD, 2023. Fiscal year 2024 program acquisition costs by weapon system.

- Dosi, G., 1982. Technological paradigms and technological trajectories: a suggested interpretation of the determinants and directions of technical change. Research policy 11, 147–162.
- Dosi, G., 1984. Technical change and industrial transformation: the theory and an application to the semiconductor industry. Springer.
- Edler, J., Blind, K., Kroll, H., Schubert, T., 2023. Technology sovereignty as an emerging frame for innovation policy. defining rationales, ends and means. Research Policy 52, 104765.
- Fanti, L., Guarascio, D., Moggi, M., 2022. From heron of alexandria to amazon's alexa: a stylized history of ai and its impact on business models, organization and work. Journal of Industrial and Business Economics 49, 409–440.
- Foster, J.B., 2014. The theory of monopoly capitalism. NYU Press.
- Franco, S.F., Graña, J.M., Flacher, D., Rikap, C., 2023. Producing and using artificial intelligence: What can europe learn from siemens's experience? Competition & Change 27, 302–331.
- Gawer, A., 2022. Digital platforms and ecosystems: remarks on the dominant organizational forms of the digital age. Innovation 24, 110–124.
- Gentile, G.P., Shurkin, M.R., Evans, A.T., Grisé, M., Hvizda, M., Jensen, R., 2021. A History of the Third Offset, 2014-2018. RAND Corporation Santa Monica, CA.
- Gjesvik, L., 2023. Private infrastructure in weaponized interdependence. Review of International Political Economy 30, 722–746.
- Gonzales, R., 2023.Militarising big tech. the sil- rise of digital icon vallev's defence industry. TNI. Available at: https://www.tni.org/en/article/militarising-big-tech, 1–12.
- Goodwin, C., 2018. Cooperation or resistance?: The role of tech companies in government surveillance. HARV. L. REV. 131, 1722–1722.
- Greenstein, S., 2015. How the internet became commercial: Innovation, privatization, and the birth of a new network. Princeton University Press.

- Greenstein, S., 2020. The basic economics of internet infrastructure. Journal of Economic Perspectives 34, 192–214.
- Griffiths, J., 2021. The great firewall of China: How to build and control an alternative version of the internet. Bloomsbury Publishing.
- Hilferding, R., 1908 [1923]. Das finanzkapital. Wien: Verlag der Wiener Volksbuchhandlung.
- Hobson, J., 1902. Imperialism, A Study. New York: James Pott and Company.
- Hötte, K., Tarannum, T., Verendel, V., Bennett, L., 2023. Ai technological trajectories in patent data .
- Hymer, S., 1970. The efficiency (contradictions) of multinational corporations. The American economic review 60, 441–448.
- Hymer, S., 1972. The internationalization of capital. Journal of economic issues 6, 91–111.
- Hymer, S.H., 1960. The international operations of national firms, a study of direct foreign investment. Ph.D. thesis. Massachusetts Institute of Technology.
- Ietto-Gillies, G., 2012. Transnational corporations and international production: concepts, theories and effects. Edward Elgar Publishing.
- Ietto-Gillies, G., 2021. Transnationality in the xxi century. concept and indicators. critical perspectives on international business.
- Ietto-Gillies, G., Trentini, C., 2023. Sectoral structure and the digital era. conceptual and empirical analysis. Structural Change and Economic Dynamics 64, 13–24.
- Jacobsen, A., 2015. The Pentagon's Brain: An Uncensored History of DARPA, America's Top-secret Military Research Agency. Hachette UK.
- Johnson, J., 2019. Artificial intelligence & future warfare: implications for international security. Defense & Security Analysis 35, 147–169.

- Keane, M., Yu, H., 2019. A digital empire in the making: China's outbound digital platforms. International Journal of Communication 13, 4624–4641.
- Kemmerling, M., Trampusch, C., 2022. Digital power resources (dpr): The political economy of structural and infrastructural business power in digital (ized) capitalism. Socio-Economic Review, mwac059.
- Kenney, M., Zysman, J., 2020. The platform economy: restructuring the space of capitalist accumulation. Cambridge journal of regions, economy and society 13, 55–76.
- Kowalik, T., 2014. Rosa Luxemburg: Theory of accumulation and imperialism. Springer.
- Kwet, M., 2019. Digital colonialism: Us empire and the new imperialism in the global south. Race & Class 60, 3–26.
- Lenin, V., 1963 [1917]. Imperialism, the Highest Stage of Capitalism. Moskow: Progress Publisher.
- Li, Z., Qi, H., 2022. Platform power: monopolisation and financialisation in the era of big tech. Cambridge Journal of Economics 46, 1289–1314.
- Lundvall, B.Å., Rikap, C., 2022. China's catching-up in artificial intelligence seen as a co-evolution of corporate and national innovation systems. Research Policy 51, 104395.
- Maaser, L., Verlaan, S., 2022. Big tech goes to war. Studien 5, 2022.
- Marx, K., 2004 [1867]. Capital: volume I. Penguin UK.
- Marx, K., Engels, F., 1967 [1948]. The communist manifesto. 1848. Trans. Samuel Moore. London: Penguin 15, 9780822392583–049.
- Maslej, N., Fattorini, L., Brynjolfsson, E., Etchemendy, J., Ligett, K., Lyons, T., Manyika, J., Ngo, H., Niebles, J.C., Parli, V., et al., 2023. The ai index 2023 annual report. AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, Stanford, CA.
- Mazzucato, M., 2018. Mission-oriented innovation policies: challenges and opportunities. Industrial and Corporate Change 27, 803–815.

- Miller, C., 2022. Chip war: the fight for the world's most critical technology. Simon and Schuster.
- Mowery, D.C., 2009. National security and national innovation systems. The Journal of Technology Transfer 34, 455–473.
- Mowery, D.C., 2010. Military r&d and innovation, in: Handbook of the Economics of Innovation. Elsevier. volume 2, pp. 1219–1256.
- Mudge, S.L., 2008. What is neo-liberalism? Socio-economic review 6, 703–731.
- O'Mara, M., 2020. The code: Silicon Valley and the remaking of America. Penguin.
- R., 2021.2021. Pub-Paulson. Tech inquiry report lic Available Information PAI. Available at: ht-_ tps://techinquiry.org/EasyAsPAI/resources/EasyAsPAI.pdf 5, 1–42.
- Paulson, R., 2022. Tech inquiry report 2022. Public Available Information - PAI, Available at: https://techinquiry.org/docs/InternationalCloud.pdf , 1–154.
- Pianta, M., 1989. High technology programmes: for the military or for the economy?, in: Making Peace Possible. Elsevier, pp. 185–217.
- Pitelis, C., 2022. Big tech and platform-enabled multinational corporate capital (ism): the socialisation of capital, and the private appropriation of social value. Cambridge Journal of Economics .
- Polanyi, K., 2015. The great transformation.
- Rahman, K.S., Thelen, K., 2019. The rise of the platform business model and the transformation of twenty-first-century capitalism. Politics & society 47, 177–204.
- Rikap, C., 2023. Same End by Different Means: Google, Amazon, Microsoft and Meta's Strategies to Organize Their Frontier AI Innovation Systems. City, University of London.
- Rikap, C., Lundvall, B.Å., 2022. Big tech, knowledge predation and the implications for development. Innovation and Development 12, 389–416.

- Rikap, C., Lundvall, B.Å., et al., 2021. The digital innovation race. Springer Books .
- Rolf, S., Schindler, S., 2023. The us–china rivalry and the emergence of state platform capitalism. Environment and Planning A: Economy and Space , 0308518X221146545.
- Sawyer, M., 2022. Monopoly capitalism in the past four decades. Cambridge Journal of Economics .
- Schmid, J., 2018. The diffusion of military technology. Defence and Peace Economics 29, 595–613.
- Schumpeter, J.A., 1972. Imperialism and Social Classes: Two Essays. Ludwig von Mises Institute.
- Shull, A., Araya, D., Bradshaw, S., Gill, A.S., Horowitz, M.C., King, M., Mazzolin, R., Medeiros, M., Nieto-Gómez, R., Vihul, L., 2020. Modern conflict and artificial intelligence.
- UNCTAD, 2019. Digital economy report 2019. value creation and capture: Implications for developing countries.
- Vasudevan, R., 2021. The network of empire and universal capitalism: imperialism and the laws of capitalist competition. Review of Social Economy 79, 76–102.
- Vasudevan, R., 2022. Digital platforms: monopoly capital through a classicalmarxian lens. Cambridge Journal of Economics .
- Wong, J., Younossi, O., 2023. Improving Defense Acquisition: Insight From Three Decades of RAND Research. Technical Report. Acquisition Research Program.
- Wu, X., 2020. Technology, power, and uncontrolled great power strategic competition between china and the united states. China International Strategy Review 2, 99–119.
- Zuboff, S., 2019. The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019. Profile books.