Coveri, Andrea; Cozza, Claudio; Guarascio, Dario

Article

Big Tech and the US Digital-Military-Industrial Complex

Intereconomics

Suggested Citation: Coveri, Andrea; Cozza, Claudio; Guarascio, Dario (2025) : Big Tech and the US Digital-Military-Industrial Complex, Intereconomics, ISSN 1613-964X, Sciendo, Warsaw, Vol. 60, Iss. 2, pp. 81-87, https://doi.org/10.2478/ie-2025-0017

DOI: 10.2478/ie-2025-0017

Forum

sciendo

Intereconomics, 2025, 60(2), 81-87

JEL: L12, L22, P12

Andrea Coveri, Claudio Cozza and Dario Guarascio

Big Tech and the US Digital-Military-Industrial Complex

Large digital platforms – Meta (Facebook), Amazon, Microsoft, Alphabet (Google) and Apple, the so-called Big Tech companies, which are compared to Chinese counterparts like Alibaba, JD or Tencent – dominate the world economy. Their market capitalisation has exceeded the GDP of large economies such as Germany or Japan.[1] They control a significant share of global research and development (R&D)[2] and patents related to frontier technologies, such as artificial intelligence (AI) (Fanti et al., 2022; Hötte et al., 2023). These figures reflect an unprecedented concentration of techno-economic power, with major implications for income distribution, access to knowledge and innovation, fragmentation and precarisation of labour, as well as on rising geopolitical tensions (Armoogum et al., 2022; Vasudevan, 2022).

At the root of this power is the control of knowledge, infrastructure (e.g. data centres, submarine cables) and, above all, dual-use technologies – i.e. cloud, AI, and new satellite navigation and communication systems – essential in both civilian and military spheres (Farrell & Newman, 2022; Coveri et al., 2024). Unsurprisingly, Big Tech companies are now key players in the clash between the two "digital-military-industrial complexes" (Guarascio & Pianta, 2025) – China and the United States – that are competing for global hegemony (Jia et al., 2018; Li & Qi, 2022; Rolf & Schindler, 2023). This is contributing to the blurring of the state-corporation boundaries even more than what was observed during the second half of the twentieth century with the rise of transnational corporations (Hymer, 1972; Cowling, 1982). In this respect, the ubiquitous role of Elon Musk within the new Trump Administration, or the loyalty shown by the other Big Tech CEOs during the swearing-in ceremony,[3] lend support to the hypothesis of a strategic convergence of interests (O'Mara, 2020; Coveri et al., 2024).

Military and intelligence apparatuses cannot do without Big Tech. The latter control tools (among them, cloud systems or AI algorithms aimed at image and sound recognition, behaviour prediction and military targeting) that are essential for surveilling adversaries (and "allies") and, if needed, to anticipate their moves on the battlefield. These corporations play a pivotal role in military-related innovation ecosystems, helping to mobilise the R&D efforts of start-ups and facilitating the transfer to the military sphere of technologies designed for the civilian domain (Gawer, 2022; Guarascio & Pianta, 2025). No less relevant, media platforms run by Big Tech – e.g. the social media platform X, owned by Elon Musk – are supportive in building political consensus and influencing public opinion, both at home and abroad.

On the other hand, public investments, particularly those aimed at buying and/or developing dual technologies, are a relevant source of accumulation for digital corporations; as well as a stimulus for their innovative activity (Coveri et al., 2022). Equally important may be government support when Big Tech internationalisation strategies are hampered by hostile governments and regulations (Kwet, 2019). In this context of "mutual dependence" (Coveri et al., 2024), the more intense the relationship between the state and Big Tech is, the less likely the former is to put restrictions in place – e.g. higher taxation, stricter antitrust measures or binding regulations aimed at limiting platforms' access to private information – that would seriously challenge the economic power of the platforms.

Building on Coveri et al. (2022, 2024), we focus on the US digital-military-industrial complex highlighting and empirically documenting the channels holding the two sides together. First, we identify the main elements shaping the interdependency between the state and Big Tech. Second, we explore military expenditures and procurement

1 See, for example, data reported by Visual Capitalist (2021) and Statista.com (2024).

2 By 2024, Big Tech's R&D investment was US $240 billion, more than a quarter of the total recorded in the United States. See Guarascio and Pianta (2025).

Open Access funding provided by ZBW – Leibniz Information Centre for Economics.

Andrea Coveri, University of Urbino, Italy.

Claudio Cozza, University of Naples Parthenope, Italy.

Dario Guarascio, Sapienza University of Rome, Italy.

3 After publicly expressing their support for the new administration, including through financial handouts, the CEOs of Alphabet, Amazon and Meta took part in the inauguration, marking a relative discontinuity from the attitude of distance from politics that has traditionally characterised Big Tech.

contracts, showing both the progressive militarisation of digital technologies, as well as the growing importance of Big Tech as military contractors. Third, we shed light on the "revolving doors" allowing former Big Tech officers to join military and intelligence agencies, and vice versa. Fourth, we document the active role of digital corporations in current war scenarios, contributing to dismantling the "don't be evil" rhetoric according to which Big Tech-controlled infrastructures and technologies are never used for malicious purposes.

Big Tech and the emergence of a digital-military-industrial complex

When John Hobson published *Imperialism* in 1902, military campaigns were crucial for opening new markets, securing the supply of raw materials and putting competitors out of business. With the consolidation of large transnational corporations, military expenditures have assumed a prominent role in sustaining capital accumulation, especially during periods of stagnation (Baran & Sweezy, 1966). Likewise, military-related R&D and procurement turn out to be important drivers of technology transfer, particularly for the development of radical innovations such as the Internet (Mowery, 2009). In the US, the linkage between military R&D agencies (e.g. the Defense Advanced Research Projects Agency, DARPA) and large private contractors is at the core of the "military-industrial complex", which was instrumental to the country's economic and technological growth during the Cold War (Galbraith, 2007).

The military sector is thus a domain where state-corporation boundaries may become significantly blurred (Pianta, 1989; Foster & McChesney, 2014; Roland, 2021). With the digitalisation of the world economy, this overlap becomes even stronger. Controlling digital networks and the "chokepoints" through which information flows from one continent to another allows for "weaponizing interdependencies" (Farrell & Newman, 2022), providing a substantial advantage over enemies and allies alike. Yet, this is virtually impossible without the support of Big Tech, as the latter controls knowledge (Rikap, 2024), technologies, such as cloud systems and AI (Van der Vlist et al., 2024), and physical infrastructures, e.g. data centres and submarine cables (Gjesvik, 2023), without which global networks can hardly be weaponised. No less relevant, contemporary wars are becoming increasingly "digital" (Merrin & Hoskins, 2020). AI-powered drones sold for less than US $100,000 can easily destroy aircrafts or tanks that are 100 times more expensive. Advanced cloud and satellite communications systems are essential for gathering information and preventing or executing attacks (physical and cyber). Even the performance of traditional weapons (e.g. aircrafts, tanks, anti-aircraft systems) is highly dependent on their digital components (Johnson, 2019; González, 2023; Zikusoka, 2024).

The digital-military-industrial complex is fairly different from the entanglement of public and private interests denounced by President Eisenhower in 1961, when the military-industrial complex was first defined. In the latter, traditional contractors (e.g. Lockheed Martin, Raytheon, Halliburton) were largely dependent on public demand and their innovative activity was closely linked to the needs of the military sector (Guarascio & Pianta, 2025). Accordingly, procurement relationships were (and to a good extent still are) characterised by large, long-term contracts; a strong focus on the performance of weapon systems (while less attention was devoted to efficiency or flexibility of use); and a high degree of bureaucratisation of processes (Pianta, 1989). This has biased technological trajectories and, in some cases, weakened the industry's ability to innovate (Kaldor, 1990). The digital-military-industrial complex operates in a rather different way. Despite owing their birth to a military project (the Internet), Big Tech earn most of their profits in the civilian domain; and a majoritarian share of the technologies that they develop for the military sector stem from applications initially designed for commercial purposes. This gives them greater bargaining power vis-à-vis government procurers, consolidating their role as exclusive providers of dual technologies and, more broadly, reducing the risk of being challenged by hostile regulations.

The interdependency between the state and Big Tech

First of all, there is an original linkage. As argued, the economic power of Big Tech stems from the appropriation of knowledge and technologies developed in the public (mostly military) sector and transferred at virtually no cost by the same governmental apparatuses that helped develop them (Mazzucato, 2013).[4] First movers, including soon-to-be Big Tech, have begun to push forward the technological frontier, introducing thousands of radical and incremental innovations, designed primarily for commercial

4 Major projects carried out by US federal agencies, such as DARPA (Mowery, 2010), contributed to the development of General Purpose Technologies (GPTs) – including semiconductors, the Transmission Control Protocol and the Internet Protocol (TCP/IP) (Greenstein, 2020) – and were crucial to the spread of computers and, later, the Internet itself (Mazzucato, 2018). In this context, close relationships between DARPA, private technology firms and the country's leading universities fostered technology transfer, incremental innovations, and forged the U.S. National Innovation System (NIS) (Freeman, 1995). With the "commercialization of the Internet" (Greenstein, 2015), few companies exploited the "first mover" advantage by gaining dominant positions in critical market segments such as search engines (Alphabet), social networks (Meta), digital marketplaces (Amazon) and cloud services (e.g. Amazon Web Services and Microsoft Azure).

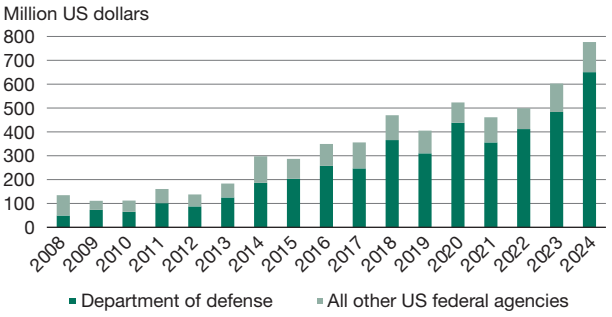
use. Although their growth takes place mainly in the civil-commercial sphere, the original linkage between Big Tech and the military apparatus never completely disappears. After the Twin Towers attack on 11 September 2001, US military and counter-terrorism policy recognised the value of digital infrastructures and technologies. As a result, Big Tech has been increasingly involved in intelligence- and military-related projects, including surveillance systems, secure communications and remote management of weapons and military equipment. The dual nature of applications designed, for instance to predict consumer behaviour (Zuboff, 2019) or optimise the functioning of logistics systems, is beginning to emerge (González, 2023).

At the same time, skills and competences stemming from the public sector are a crucial source of knowledge to develop Big Tech's R&D projects (Rikap & Lundvall, 2022). On the demand-side, the Department of Defense (DoD) budget for digital technologies kept growing. In the fiscal year 2024 budget, DoD requested US $315 billion for weapon systems acquisition, an increase from US $276 billion in 2023. This includes US $170 billion for procurement and US $145 billion for research, development, test and evaluation (R&DTE). Digital technologies play a central role in R&DTE efforts, with significant funding increases for cyberspace, spectrum, AI, 5G, and other digital-related programmes (Coveri et al., 2024). Moreover, investment in command, control, communications, computers and intelligence (C4I) – a field heavily reliant on digital technologies – has experienced the fastest growth among DoD budget components. Funding increased from US $7.4 billion in 2017 to US $12.8 billion in 2023 and is projected to reach US $21 billion in 2025.[5] This budget covers command centres, data processing, IT infrastructure, communication systems, air traffic control, night vision equipment and cyberspace operations. Additionally, science and technology (S&T) activities will receive US $18 billion in 2025, with priorities focusing on AI and machine learning applications, 5G, microelectronics, quantum sciences, cyberwarfare, hyper-sonics, directed energy weapons (such as lasers and particle beams), biotechnology and space technologies.

Regarding military-related procurement contracts awarded to Big Tech, we showed how the former increased about thirteenfold from 2008 to 2024. To illustrate, Figure 1 reports the value of contracts awarded to Big Tech, highlighting the share of resources stemming from the DoD.

Compared to the overall revenues of Big Tech, the value of these contracts is obviously small. Yet, these figures likely underestimate the real numbers, as many military and intelligence-related projects are classified (González, 2023). What truly matters, however, is the role that Big Tech play in managing critical infrastructure and technologies. Accordingly, Table 1 reports a selection of multi-year contracts that DoD, the Central Intelligence Agency (CIA) and National Security Agency (NSA) award Big Tech, providing details on the amounts, nature of the services delivered, and their intended military or intelligence applications.

Figure 1
US Federal procurement contracts awarded to Alphabet, Amazon, Meta and Microsoft, 2008-2024



Source: Adapted from Coveri et al. (2024).

In 2013, the CIA awarded Amazon Web Services (AWS) a 10-year contract, worth a total of US $600 million, to provide cloud computing services to all 17 US intelligence agencies. In 2014, AWS launched its first "Top Secret Region", called "Top Secret-East", which was followed by the launch of a second, known as "Top Secret-West", providing cloud services for US intelligence and defence agencies (including the NSA). Microsoft has been providing similar services under the "Azure Government Secret" projects, launched in 2017, and "Azure Government Top Secret", introduced in 2021.

Other relevant initiatives include: *Project Maven*, launched by the DoD in 2017 and involving first Google and later Amazon and Microsoft, aimed at developing surveillance software embedded in military drones; *Commercial Cloud Enterprise*, contracted in 2020 by the CIA with AWS, Alphabet, IBM, Microsoft and Oracle to provide cloud services; *Wild and Stormy* (worth US $10 billion), awarded by the National Security Agency (NSA) to AWS in 2022 and aimed at transferring US intelligence data from internal servers to Amazon's cloud infrastructure; *Joint Warfighting Cloud Capability (JWCC)*, awarded in 2022 by the DoD to Amazon, Google, Microsoft and Oracle (the economic value was disclosed to be about US $9 billion) for strengthening the military cloud.

5 Detailed information can be found at comptroller.defense.gov/Portals/45/Documents/defbudget/FY2024/FY2024_Budget_Request_Overview_Book.pdf.

Table 1
Selection of military contracts assigned by DoD, CIA and NSA to US digital corporations (2013-2024)

Year	Department	Contractor	Amount (million US $)	Nature of activities	Stated objective
2013	CIA	Amazon	600	Cloud	Data management aimed at preventing terrorist attacks
2019	DoD ("Project Maven")	Alphabet (withdrawn); Amazon and Microsoft	50	Drones	Acquisition of AI technologies to improve image recognition in military drones
2020	CIA ("Commercial Cloud Enterprise")	Alphabet, Amazon, Microsoft and Oracle	"Tens of billions"	Cloud	Cloud services centralised for 17 intelligence agencies
2021	DoD (HoloLens)	Microsoft	21,9	Augmented reality visors	HoloLens augmented reality headset for military activities in highly complex environments
2022	NSA ("Wild and Stormy" project)	Amazon	10	Cloud	NSA cloud infrastructures
2022	DoD	Microsoft	n.a.	Stryker armoured vehicles	Digital tools to be embedded into armed Army vehicles
2022	DoD	Alphabet (Google public sector division)	n.a.	Google workspace	Provision of Google Workspace to 250,000 DoD employees
2022	DoD ("Joint Warfighting Cloud Capability")	Alphabet, Amazon, Microsoft and Oracle	9	Cloud	Defense cloud infrastructure
2022	DoD ("Hybrid Space Architecture" program)	Amazon and Microsoft	n.a.	Satellites	Space and land infrastructure for national security
2022	DoD	Amazon	724	Cloud	Cloud services to process and store data for critical missions
2023	Space Systems Command / DoD	Microsoft	19.8	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	Cloud	Cloud services for the Army department of the US Special Operations Command

Source: Adapted from Coveri et al. (2024).

AWS also contributed to the development of the first permanent tactical cloud for the US Army's XVIII Airborne Corps, as well as the launch of AWS Modular Data Center and AWS Snowblade. The latter are devices made available to the DoD to enable the Army to collect, store and process data in remote or high-risk warfare contexts. Finally, in addition to cloud technologies and infrastructure, the Pentagon acquired 120,000 HoloLens augmented reality visors, developed by Microsoft – based on a 2021 contract worth nearly US $22 billion – that were aimed as much at equipping soldiers as at being incorporated into Stryker armoured vehicles.

Why is this evidence so relevant? By overseeing data centres, cloud services, submarine cables, AI systems designed to prevent cyberattacks and infrastructures that ensure connectivity in conflict zones, Big Tech has become the eyes and ears of governments both at home and abroad (Coveri et al., 2024). This allows them to access sensitive information and develop specific competences that may further strengthen their position vis-à-vis national governments. Moreover, the possibility of experimenting with new technologies in extreme and barely regulated contexts such as battlefields provides such corporations with a unique opportunity to perfect and refine new applications. In this respect, it is interesting to note that many companies producing AI technologies emphasise their role as military contractors as a way to highlight their reliability and technological ingenuity.[6]

6 A case in point is the war in Gaza, where digital companies – including many US Big Tech firms – have rushed to offer the Israeli military the latest advances in the field of AI. See, for example, https://www.washingtonpost.com/technology/2025/01/21/google-ai-israel-war-hamas-attack-gaza/.

Revolving doors

The increasingly close relationship between Big Tech and the military sector can also be highlighted by looking at the "revolving doors" already documented during the Cold War (Brunton, 1988; Etzion & Davis, 2008; Duncan & Coyne, 2015). This is about the movement of a growing number of senior Big Tech executives into military and intelligence agencies, while former members of the military apparatus are appointed to hold top roles in the same companies.

These movements allow the military sector to leverage skills and networks of relationships that can be crucial to monitor the technological frontier to identify, in a timely manner, the most promising applications (Lundvall & Rikap, 2022). By the same token, former military and intelligence personnel can help Big Tech to anticipate demand-side needs, better tailoring digital applications and circumventing the bureaucratic constraints that often slow down diffusion and technology transfer. Relatively recent examples include the former Apple Vice President Doug Beck, who was recently appointed as the new director of the Defense Innovation Unit;[7] and the Alphabet's former CEO Eric Schmidt, who served – along with former Secretary of State Henry Kissinger and former Deputy Secretary of Defense Robert Work – as Chairman of the Defense Innovation Advisory (DIA) Board and the National Security Commission on AI, namely advisory bodies aiming to counter China's growth in the development of dual (digital) technologies. As for the movements from the military apparatus to Big Tech, notable cases include former DIA Executive Director Josh Marcuse, who in 2020 took a management role within Google Public Sector, i.e. the Google's department that develops technologies for government agencies, including those related to the military; and General Keith Alexander, former director of the NSA from August 2005 to March 2014 and commander of US Cyber Command from May 2010 to March 2014, who joined Amazon's board of directors in September 2020.[8]

Big Tech goes to war

Finally, the digital-military-industrial complex manifests itself with the direct involvement of Big Tech in ongoing conflicts. In Ukraine, in addition to the major role played by Space-X, Elon Musk's company providing Internet connectivity to the Ukrainian army through its low-orbit satellite system, AWS and Microsoft have been managing the IT infrastructure of the Ukrainian public administration and banking system since the very early stages of the conflict (González, 2023; Coveri et al., 2024). Big Tech has been providing cloud and AI services to the Israeli army in its war in Gaza. More specifically, since 2021, the US $1.2 billion Nimbus project ties Alphabet and Amazon to the Israeli government for the provision of AI-based facial recognition and object tracking systems. The latter have played a prominent role in the military campaigns conducted in Gaza since October 2023. In 2024, Google agreed on an extension of the partnership to provide Israel's Ministry of Defence with additional cloud services.

As argued, access to conflict areas provides platforms with a unique test-bed for testing, evaluating and adapting new technologies. Accordingly, the battlefield becomes a peculiar laboratory that allows for experimentation, testing and refinement of military technologies that, in some cases, may prove transferable and profitable in the civilian domain as well (Fox & Probasco, 2022; Bergengruen, 2024). At the same time, as Big Tech becomes essential partners in conducting an increasing number of military activities, the government tends to build stable alliances with these companies. Again, the current Trump-Musk liaison could be considered a piece of evidence supporting such hypothesis.

Conclusions

The link between Big Tech and the military apparatus brings back traditions of economic thought too often forgotten or intentionally removed, such as the twentieth century theories of imperialism and monopoly capital (Hobson, 1902; Baran & Sweezy, 1966). The debate on the military-industrial complex, a concept associated with President Eisenhower's farewell address in 1961, also regains relevance. However, it seems to have been transformed into a digital-military-industrial complex where the key actor, Big Tech, share the peculiarity of being, at the same time, big market players, controllers of technologies essential to citizens' lives and indispensable partners of the military apparatus. This makes the integration of state and private capital even closer and more complex than in the past. It is in this context that the interdependence between the state and Big Tech is forged: a relationship in which the interests of the state prove at times indistinguishable from those of Big Tech, as the latter dominates the infrastructure, technologies and knowledge necessary for the economic, political and military survival of contemporary societies.

7 The Defense Innovation Unit – launched in 2015 by then Secretary of Defense Ash Carter – is a new US agency tasked with engaging digital corporations in the development of defence projects, narrowing the gap between the military and frontier commercial technologies (Kaplan, 2016).

8 Other notable cases involve revolving doors between defence-related government agencies and Google divisions, particularly Google Public Sector. According to the Tech Transparency Project, from 2006 to 2016, 258 such instances occurred between Google and US federal agencies, including the CIA and other security agencies. See Google's Revolving Door (2016).

The relationship between Big Tech and the military apparatus is not free of contradictions, however. Orienting an increasing part of R&D activities toward military objectives may negatively bias the innovative strategy of these corporations, reducing their interactions with the civilian domain, where a significant part of incremental innovations is developed; and weakening the organisational flexibility required by learning processes along the technological trajectory (Pianta, 1989). In the medium to long run, this may result in a weakening of the innovative capacity of Big Tech, which may find itself involved in extremely expensive but technologically unrealistic projects, as happened during the 1980s with the Strategic Defense Initiative (or Star Wars) launched by Ronald Reagan (Guarascio & Pianta, 2025).

Moreover, the close relationship with the military apparatus may give rise to conflicts between executives (inclined to meet the demands of their government counterparts) and workers, eventually unwilling to employ their skills to pursue military objectives. In April 2024, dozens of Alphabet engineers were fired for opposing the aforementioned Nimbus project, which involves the Israeli military's use of technologies developed by the company (similar protests took place within Amazon). Similarly, in 2018, more than 3,000 Google employees signed a petition against the company's involvement in the aforementioned Project Maven. This led to Google's abandonment of the project (quickly replaced by Microsoft and Amazon), although its venture capital wing (Google Ventures) retained stakes in at least two companies supplying military surveillance tools (Orbital Insight and Planet) to both the DoD and the National Geospatial-Intelligence Agency (NGA). The DoD "turned over" the management of Project Maven to the NGA in 2022.

The interdependence between the state and Big Tech that we have documented challenges the traditional distinction between the state and the market, blurring their boundaries and, most importantly, questioning the willingness (and ability) of the former to control (and discipline) the latter in the collective interest. This should not come as a surprise: as we have shown, Big Tech turns out to be increasingly important both for winning today's fierce intercapitalist competition, as well as for winning the wars that such competition continually threatens to trigger.

In such a framework, instruments such as antitrust policies can do little against the power of these large corporations, if only because the fines imposed on them are smoothed out with the turnover of a few days, if not hours. Rather, it would be necessary to question the private monopoly of knowledge and infrastructure that underlies this power, as well as the intermingling of interests that exists between them and the expansionist aims of their governments.

Europe faces considerable difficulties in this context. Its technological deficit in the digital domain makes it highly dependent on the US digital-military complex. Apart from the non-trivial attempts to curb the power of Big Tech through antitrust measures or via the introduction of regulations aimed at limiting the access to personal data (e.g. the General Data Protection Regulation, GDPR), European citizens, companies and member states do not yet have much of an alternative but to rely on the digital services offered by Big Tech. In this respect, the arms race that the EU is launching risks further strengthening the digital-military complex, thus increasing rather than reducing such dependency.

Europe should put forth an alternative to such a dangerous convergence between the power of big corporations and the militarisation of digital technologies. It is not inevitable to use such technologies for conditioning consumers' behaviour, surveillance, or to make war. Nor is it inevitable that the control and development of digital technologies ends up in seemingly unbreakable private monopolies, contributing to the growth of inequalities and the weakening of democratic systems. On the contrary, in the context of a rediscovered industrial policy, the EU should work towards building public digital platforms that contribute to direct research and innovation efforts towards the pursuit of collective interests (e.g. expanding the supply of public goods such as health and education) and not towards strengthening systems of repression and war. Accordingly, the system of rules put in place by policies such as the GDPR or the AI Act[9] should be consolidated, not weakened in the name of competitiveness, as the Draghi report seems to suggest (Draghi, 2024).

Even more important, however, is the need to rethink the private nature of the Internet, which seems to have betrayed its initial promises: not the expected vector of widespread economic opportunities and democratic empowerment, but a driver of commodification, concentration of techno-economic power and geopolitical tensions.

9 https://digital-strategy.ec.europa.eu/en/policies/ai-pact

References

Armoogum, P., Davies, S., & Mariuzzo, F. (2022). The changing face of anti-trust in the world of Big Tech: Collusion versus Monopolisation. *Cambridge Journal of Economics*, *46*(6), 1455–1479.

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

Bergengruen, V. (2024, February 8). How Tech Giants Turned Ukraine Into an AI War Lab. *Time Magazine*.

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

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

Coveri, A., Cozza, C., & Guarascio, D. (2024). Blurring Boundaries: An Analysis of the Digital Platforms-Military Nexus. *Review of Political Economy*, 1–32.

Cowling, K. (1982). *Monopoly Capitalism*. Macmillan.

Draghi, M. (2024). *The future of European competitiveness – In-depth analysis and recommendations*. European Commission.

Duncan, T. K., & Coyne, C. J. (2015). The Revolving Door and the Entrenchment of the Permanent War Economy. *Peace Economics, Peace Science and Public Policy*, *21*(3), 391–413.

Etzion, D., & Davis, G. F. (2008). Revolving Doors? A Network Analysis of Corporate Officers and U.S. Government Officials. *Journal of Management Inquiry*, *17*(3), 157–161.

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

Farrell, H., & Newman, A. L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*, *44*(1), 42–79.

Foster, J. B., & McChesney, R. (2014). Surveillance Capitalism. *Monthly Review*, *66*(3), 1–31.

Fox, C. H., & Probasco, E. S. (2022, October 19). Big Tech Goes to War. To Help Ukraine, Washington and Silicon Valley Must Work Together. *Foreign Affairs*.

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 University Press.

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

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.

Google's Revolving Door. (2016, April 26). *Tech Transparency Project*.

Greenstein, S. (2015). *How the Internet Became Commercial: Innovation, Privatization, and the Birth of a New Network*. Princeton University Press.

Greenstein, S. (2020). The Basic Economics of Internet Infrastructure. *Journal of Economic Perspectives*, *34*(2), 192–214.

Guarascio, D., & Pianta, M. (2025). Digital technologies: civilian vs. military trajectories. *LEM Working paper series.*

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

Hötte, K., Tarannum, T., Verendel, V., & Bennett, L. (2023). AI Technological Trajectories in Patent Data: General Purpose Technology and Concentration of Actors. *INET Oxford Working Paper*, 2023-09.

Hymer, S. (1972). The multinational corporation and the law of uneven development. In J. N. Bhagwati (Ed.), *Economics and World Order: From the 1970's to the 1990's* (pp. 113-140). Macmillan.

Jia, K., Kenney, M., & Zysman, J. (2018). Global Competitors? Mapping the Internationalization Strategies of Chinese Digital Platform Firms. In R. van Tulder, A. Verbeke & L. Piscitello (Eds.), *International Business in the Information and Digital Age*. Emerald Publishing Ltd.

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

Kaldor, M. (1990). Research, Development and Production: The Baroque Arsenal in Perspective. In S. Feldman (Ed.), *Technology and Strategy: Future Trends*. Routledge.

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

Li, Z., & Qi, H. (2022). Platform Power: Monopolisation and Financialisation in the era of big Tech. *Cambridge Journal of Economics*, *46*(6), 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*(1), 104395.

Kaplan, F. (2016, December 19). The Pentagon's Innovation Experiment. *MIT Technology Review*.

Mazzucato, M. (2013). *The Entrepreneurial State: Debunking Public vs. Private Sector Myths*. Anthem Press.

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

Merrin, W., & Hoskins, A. (2020). Tweet Fast and Kill Things: Digital War. *Digital War*, 1, 184–193.

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 B. Hall & N. Rosenberg (Eds.), *Handbook of the Economics of Innovation* (Vol. 2., pp. 1219–1256). Elsevier.

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

Pianta, M. (1989). High Technology Programmes: For the Military or for the Economy? In L. Dumas & M. Thee (Eds.), *Making peace possible. The promise of economic conversion* (pp. 185–218). Pergamon Press.

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

Rikap, C., & Lundvall, B.-Å. (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*. Johns Hopkins University Press.

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

Statista.com. (2024). *Leading tech companies worldwide 2024, by market capitalization*.

van der Vlist, F., Helmond, A., & Ferrari, F. (2024). Big AI: Cloud infrastructure dependence and the industrialisation of artificial intelligence. *Big Data & Society*, *11*(1), 1–16.

Vasudevan, R. (2022). Digital Platforms: Monopoly Capital Through a Classical-Marxian Lens. *Cambridge Journal of Economics*, *46*(6), 1269–1288.

Visual Capitalist. (2021). *The World's Tech Giants, Compared to the Size of Economies*.

Zikusoka, D. (2024, February 2). Spying From Space: How a Surge in Satellites Will Revolutionize Intelligence. *Foreign Affairs*.

Zuboff, S. (2019). *The Age of Surveillance Capitalism*. Public Affairs.