The US national security state and Big Tech: frenemy relations and innovation planning in turbulent times.

Author:

Dr. Cecilia Rikap

Affiliations:

- Institute for Innovation and Public Purpose, University College London
- Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET).

Email:

c.rikap@ucl.ac.uk

Keywords

US National Security State; Big Tech; innovation planning; artificial intelligence; corporate-state diplomacy

JEL Codes

O21; O33; O34; O38.

Funding:

This contribution was not supported by any specific funding.

The US national security state and Big Tech: frenemy relations and innovation planning in turbulent times.

Abstract

I analyze the relation between what Weiss (2014) dubbed the United States National Security State (US NSS) and US Big Tech focusing on artificial intelligence (AI). I argue that the US NSS was an innovation planner until the 1990s and advance the hypothesis that, amid that empty space, this millennium has seen the emergence of AI planning by US Big Tech. This has resulted in tensions with the US NSS given the centrality of AI for the military-industrial complex and ultimately for buttressing American primacy, which has always been the US NSS's main goal. Amid today's global turbulence, this tension has leaned towards a strategic yet asymmetric alliance that I define as a frenemy relation. Beyond the tit-for-tat between the US NSS and Big Tech companies, their experiences as innovation planners open space for prefiguring an alternative, a democratic way of planning innovation for the common good.

1. Introduction

By early April 2024, the United States Department of Defense (US DoD) got a new Chief Digital and Artificial Intelligence Officer: Radha Plumb, currently deputy undersecretary of Defense for acquisition and sustainment. Before joining the US DoD, Plumb was Director of Research and Insights for Trust and Safety at Google. She had also previously worked as the Global Head of Policy Analysis at Facebook (now Meta), basically a senior management position in the lobby department.

The entanglement of the US DoD and US Big Tech is much deeper and convoluted than revolving doors. Here, I focus on artificial intelligence (AI) to elaborate on their relationship amid the harshening of global turbulence. AI not only powers search engines, fraud detection, recommendation, pricing and other commercial systems, but also surveillance and weapons.

> "The latest advancements in data, analytics, and artificial intelligence (AI) technologies enable leaders to make better decisions faster, from the boardroom to the battlefield. (…) The NDS also describes the need for the United States to sustain and strengthen deterrence against the People's Republic of China and other strategic competitors, which have widely communicated their intentions to field AI for military advantage" (US Department of Defense, 2023).

Like other leading technologies in the past, from nuclear energy to semiconductors and the internet, AI is today the key military and national security technology. In the words of Streeck (2024), the war is AI's most demanding testing ground. Yet, as I explain in Section 2, while the development of the former technologies was planned by what Weiss (2014) defines as the US National Security State (NSS), frontier AI is being planned by US Big Tech companies. Their main aim when steering and controlling the development of cutting-edge AI is to reinforce their global dominance and accumulation, which may not always be in line with the US NSS priorities.

Simultaneously, as the organizations controlling the whole AI stack, Big Tech became privileged contractors of the US military-industrial complex, as I show in Section 3. Profiting from this complex is only a tiny piece of what Big Tech gains with conflict and unrest. These corporations have fueled -if not directly contributed to turning on- the fire. By portraying China as a major

threat for the US and Western democracy at large, US Big Tech companies promote policies that reinforce their control of the whole AI stack and set the tone of AI regulations. The world's turmoil benefits them as long as it distracts regulators and the public opinion.

Section 4 conceptualizes the interplay between these corporate giants and the US NSS as a frenemy relation. At a time of heightened war tensions, the NSS technological needs expanded as Big Tech were searching for stronger alliances within the US state that could operate as a shelter from antitrust suits. I finish in Section 5 emphasizing that planning has been essential for major technological change. This opens the space for thinking of democratic planning of AI and other technologies for the common and planetary good.

2. Planning innovation

2.1. The US National Security State as the planner

Since the Second World War, the Pentagon, and afterwards the US NSS, through the central role of specific agencies like DARPA, the CIA and other agencies outside the US DoD that pursued national security objectives operated as a "strategic engine of innovation" (Weiss, 2014, p. 7). The US NSS did not merely promote and invest in risky and major research and development (R&D) moonshot projects, as it is widely known. Weiss's (2014) detailed description of the US NSS as well as other studies on the same topic (Block, 2008; Mazzucato, 2013; Phillips & Rozworski, 2019) explicitly or implicitly portray the US NSS as planning innovation, seen as an integral part of the military strategy.

Planning, can be broadly defined as the direct a priori allocation of resources for achieving a pre-defined purpose (Mandel, 1986, p. 6). Speaking of planning innovation may seem an oxymoron given the rooted common sense association of innovation with serendipity, thus with the idea that discoveries are made by chance, ergo unplanned. Weiss (2014, p. 94) herself laments that, regardless of the well-documented cases giving testimony of the contrary, "the idea of serendipity retains its appeal—presumably because it resonates with the antistatist mindset". Against common sense, the Manhattan Project can be seen as a landmark case that paved the way for an institutionalized planning of innovation led by the NSS.

> "The central hotbed of publicly planned innovation was the postwar Pentagon, coordinating government agencies that would prove responsible for the initial development of computers, jet aircraft, nuclear energy, lasers, and, contemporarily, much of biotechnology" (Phillips & Rozworski, 2019, p. 61).

The existence of multiple agencies shall not be conflated with lack of coordination. They operated in complementary ways, taking distinct roles and participating in different stages of the selected projects under the directives of the Pentagon and ultimately the US president and Congress. Having multiple agencies also unlocked more policy experimentation contributing to a faster learning by doing. In such a decentralized but coordinated manner, the US NSS planned a national technology enterprise in which technology was co-developed with private actors but governed by the US NSS. This is what Weiss (2014) describes as governed interdependence because the NSS defined the guidelines, priorities and overall directionality of technological change. Its purpose was the systemic reinforcement and expansion of the US (military) dominance aimed at sustaining American primacy by planning science and innovation. American primacy was

supposed to make democracy the universal political norm, something that seen from the present simply never happened (Skidelsky, 2024).

The US NSS agencies designed the mechanisms that would ensure the private sector compliance. Block (2008, p. 172) explains that US firms already had strong innovation incentives. Policies aimed at incentivizing them would not spur innovation further. Thus, the US state assumed a "hands on" role; it worked "closely with firms to identify and support the most promising avenues for innovation". As described by Phillips and Rozworski (2019, p. 59), the US government not only poured money but also planned technological change by identifying and strategically investing in research that could lead to major breakthroughs.

The semiconductors industry is a prominent example of the NSS strategy to assure military innovation by promoting dual-use technological change, understood as technologies with military and commercial applications. In a chapter called "Beyond Serendipity: Procuring Transformative Technology", Weiss (2014) provides a thorough assessment of the concrete ways in which the US NSS planned innovation. The chapter starts with a Reagan quote from 1983 in which he claims that technological change is not the result of luck but of investing in time, money and effort. This chapter offers plenty of evidence supporting the thesis of the US NSS planning the development of semiconductors.

> "Motivated by reports of Soviet advances in integrated circuitry, program planners sought the collaboration of semiconductor manufacturers to design circuits for DoD. Support of leading U.S. firms was won on the basis of extensive industry input into program planning, thereby holding out the hope of commercially relevant advances in a range of process technology areas" (Weiss, 2014, p. 91).

Two major technology programs were launched: the US DoD's VHSIC (Very High Speed Integrated Circuit) and DARPA led the VLSIC (Very Large Scale Integrated Circuit). Their aim was "to reassert NSS influence over the direction of technology development by offering industry the prospect of commercial payoffs", which combined R&D funding and public procurement (Weiss, 2014, p. 92). By remaining the semiconductors industry's main customer for years, a story that was reconstructed in greater detail recently (Miller, 2022), the US NSS nurtured and sustained an industry that today ranks among the world's most profitable ones.

Besides semiconductors, the US NSS set a comprehensive research agenda that was promoted by granting targeted funds for moonshot projects in computer science and technology, including the provision of funds to create computer science departments in US leading universities. This was followed, in 1980, by the Stevenson–Wydler Technology Innovation Act that mandated federal research laboratories to establish technology transfer offices and the Bayh-Dole Act, which authorized patenting publicly-funded research outcomes.

Since the 1980s, the nurturing of commercial applications together with military uses, as in the successful VLSIC, became intrinsic to the US NSS strategy. The development of new technologies that could be sold broadly beyond the US military was expected to further stimulate businesses to innovate and expand their commitment with R&D. This would reduce reliance on public R&D funding, at a time of intensified public budget pressures. The NSS, continues Weiss (2014, p. 178), boosted "commercial innovation in a deliberate and purposive manner" but not for the promotion of economic competitiveness itself but for buttressing "the primary NSS endeavor, which has been to ensure the superior technology essential to sustaining American primacy".

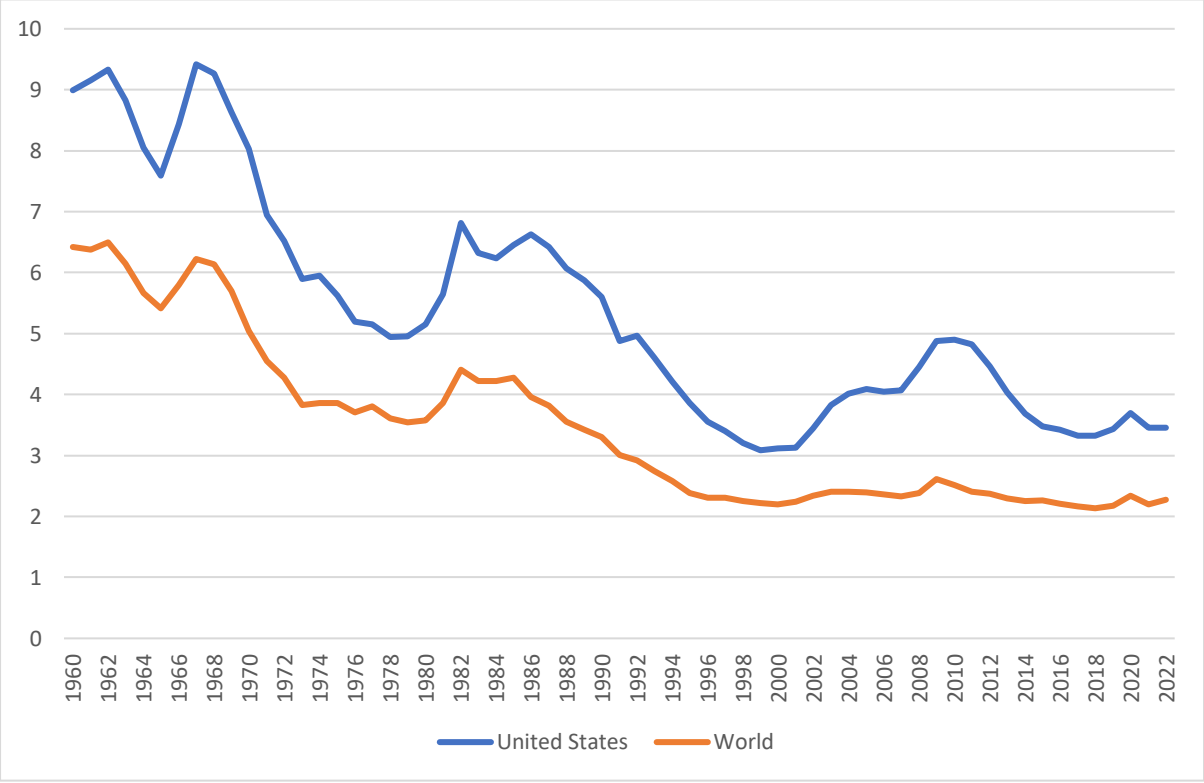
Since the dual-use strategy privileged commercial viability, the NSS influence on science and technology went way beyond security industries. The US NSS convinced information technology

companies, which had been mostly reluctant to conduct R&D for the military, to accept NSS contracts. Because of this comprehensive scope of innovation planning by the US NSS, Weiss (2014, p. 195) concludes that the "pursuit of defense preparedness, driven by Cold War exigencies and threat perceptions, produced a national security state much broader and more encompassing than the 'defense sector', responsible for mobilizing the nation's science and technology resources".

2.2. The demise of the US NSS as a planner

The end of the Cold War signaled that the US had won the technological -and political- race, which probably influenced the demise of the US NSS's innovation planning in the 1990s. If dual-use initiatives were already underfunded in the 1980s, military budgets shrank even more. As a share of GDP, the world and the US military expenditure exhibit a clear downward trend up to the present (see Figure 1).

Figure 1. Military expenditure (% of GDP)



Source: World Bank data

The relative importance of the US military budget in the world also fell. Since 2010, according to data from the World Bank, the US military expenditure represented on average 40% of the world's military expenditure. This average was 50% in the 1980s, 43% in the 1990s and 45% in the 2000s. In the meantime, China's military expenditure grew from less than 2% in 1989 to over 13% of the world's military expending in 2022.

Analyzing the reasons for this change, Ruttan (2006) recalls that military procurement had been mostly channeled to the manufacturing sector, whose place in the US economy had already been declining. Thereby, the relative importance of military contracts influencing the US economy fell

to less than half of its 1985 peak. Against this backdrop, Ruttan (2006, p. 22) observes a decrease in the incentives "to make long term investments in defense and defense related 'big science' and "big technology"" influenced by defense intellectuals who believed that interstate wars among core states were over. This resulted, continues the author, in a lack of coherently designed institutions for the development of new general purpose technologies with the sole exception of R&D in molecular genetics and biotechnology.

This decrease is the US military budget for R&D and more generally the fall in US military budget can be seen as an expression of shifts in the US economy beyond those that the termination of the Cold War triggered. By the end of the millennium, the US current account deficit with the rest of the world skyrocketed[1], which represented less available funds for long term (military) R&D bets. Coveri et al. (2023) analyze data on government budget allocations for R&D (GBARD) for Defense from 1995 to 2021 as a percentage of total GBARD. The authors highlight that the share of US GBARD for Defense is much higher than for other core OECD economies. However, they overlook the US trend itself, which decreases since the late 1990s.

In the meantime, business expenditure on R&D kept growing. As Professor Derrick J. Neal from the Defence Academy of the United Kingdom laments in a US Army Press publication, "the fact that most innovation now takes place in the private sector is particularly important, and this combines with the fact that for most developed nations, the idea of a growing defense budget is a thing of the past" (Innovative Learning: A Key to National Security p. 155). Along the same lines, Chuck Hagel, back then the US Defense Secretary, declared in the announcement of the Defense Innovation Initiative on May 2015: "We all know that DoD no longer has exclusive access to the most cutting-edge technology or the ability to spur or control the development of new technologies the way we once did".[2] The recognition of the US NSS as no longer planning innovation is also implicit in the DoD (2018, p. 12) observation that "today, the U.S. private sector and academic institutions are at the forefront of modern AI advances", which is why their AI strategy emphasizes the need to partner with them.

Besides partnering with the private sector, in the 2000s, the US NSS became a venture capitalist, taking equity positions in chosen innovating companies. In-Q-Tel, the CIA's venture capital arm was launched in 1999. Public venture capital was expanded during the 2000s to the US Army, the Department of Energy, the NASA and the DoD (Wade, 2017; Weiss, 2014). It was expected that, just like public procurement, venture capital could operate as an instrument for planning technological change favoring those projects that could simultaneously yield military and commercial applications. But, as I show next for the case of AI, public venture capital is marginal when compared to Big Tech investments in AI start-ups. Overall, Amazon and Google together spend in internal R&D more than the US Government budget allocations for R&D for Defense.[3]

2.3. Big Tech planning AI

In a Foreign Affairs piece, Google's former CEO and Chairman Eric Schmidt (2023) vocally claimed "innovation power underlies military power". He continued arguing that innovation power is not

[1] See data: https://data.worldbank.org/indicator/BN.CAB.XOKA.CD?locatios=US

[2] http://www.defense.gov/news/newsarticle.aspx?id=123651

[3] In 2022, Amazon invested in Technology and Content USD 56.052 billion and Alphabet dedicated USD 31.562 billion to R&D. Meta followed with USD 24.655 billion. In comparison, the US Government budget allocations for R&D for Defense was USD 78.361billion.

simply a country's "mastery of a given technology" but the "ability to continuously innovate." AI has put that innovation pace on steroids albeit controlled by and disproportionately benefiting a few US Big Tech. It is precisely the control of systems of continuous innovation with a resulting concentration of associated rents what characterizes intellectual monopolization.

Around two decades before Schmidt's piece, Boldrin and Levin (2004, p. 328) had defined intellectual monopolies as "the power of producers of ideas to control how their products are used". Pagano (2014) built on this definition and coined the term intellectual monopoly capitalism referring to the enlargement and harshening of intellectual property rights (IPRs) and the inclusion of knowledge among the capital assets of the firm. On this basis, Rikap (2021) showed that global corporations capture knowledge developed with other organizations and shape the trajectories of scientific exploration and technological change. Hence, intellectual monopolies are not necessarily the producers of the ideas, as in Boldrin and Levin's (2004, p. 328) definition, but those that systematically capture and turn into assets knowledge and information that is often co-produced with (and sometimes simply produced by) others. This leads to a distinction between control and ownership. The intellectual monopoly controls a corporate innovation system integrated by legally independent organizations co-creating knowledge for its benefit (Rikap & Lundvall, 2021).

Under intellectual monopolization a firm keeps turning continuously co-produced knowledge into intangible assets by leveraging on its previously captured intangibles. In other words, what Schmidt refers to as innovation power is what many have been critically studying as the rise of intellectual monopolies (see also Baines & Hager, 2023; Durand & Milberg, 2020; Rabinovich, 2023). These corporations not only siphon value from society in the forms of sustained intellectual rents but also curtail knowledge diffusion stifling complementary innovations that could distribute part of the benefits of technological change.

This dynamic is epitomized by Big Tech and AI. Contemporary AI certainly builds on decades of past developments but there has been a breaking point in 2012 that signaled the emergence of large-scale AI based on deep learning and neural networks (Rikap & Lundvall, 2021). The resulting AI stack, composed of several layers that include frontier digital infrastructure and tons of data is controlled by Microsoft, Amazon and Google joined by Meta in some of the layers.

Data on leading AI conferences show that Microsoft and Google, followed by the other two giants, are at the center of the AI research field. They even sit prominently in conferences' organizing committees, thus deciding what research is presented and awarded prizes. Their centrality in the network of organizations presenting in these conferences is indicative of Big Tech's capacity to steer the AI frontier by influencing organizations that are not directly collaborating with them (Rikap, 2023c).

Another chief space of AI co-production is the open source environment. Big Tech companies often open source some of their solutions. These are pieces of larger puzzles that only make sense once they are coupled with pieces kept secret by Big Tech. Open source offers them several advantages: 1) code gets improved by developers that are not their employees, 2) it increases employees satisfaction because they feel they are contributing to the community and 3) it enables selling complementary products or, even more profitable, creating an ecosystem on top of the open sourced solution. By controlling necessary complements, Big Tech expands control and profits. Examples abound, from Google's Android to Meta's LLMs. Big Tech expectation is to reinforce their leadership by turning their open source solutions into industry standards. This strategy is not simply a side-line story of how open source evolves. The most popular projects on

open source platforms like GitHub come from Big Tech (Rikap, 2023c; Rikap & Lundvall, 2021). This points to Big Tech control of the whole community.

Besides research and coding spaces, AI commercial products are mostly development either by Big Tech themselves or by start-ups. In 2023, Google, Microsoft and Amazon poured more money into the AI start-up world than any venture capitalist. Together, they invested two-thirds of the USD 27 billion raised.[4] In terms of the number of funded AI start-ups, by February 2024, Google was third (136 AI start-ups declared it among their top 5 investors) and Microsoft 10th (50 AI start-ups) when looking at all the companies that received venture capital funds since ChatGPT was released.[5] Precisely speaking of ChatGPT, Microsoft's backing of OpenAI since 2019 illustrates how funding AI start-ups is a means to access and steer their technologies (Rikap, 2023b). As AI start-ups assume the risks of developing a frontier technology, Big Tech retains control of the field and reaps the profits.

In comparison, the US state appears less prominently in the ranking, led by the National Science Foundation, the National Institutes of Health and the US Department of Energy with 44, 11 and 9 companies declaring them among their top 5 investors. Investments from the US NSS are almost marginal. The CIA's In-Q-Tel was only linked to 5 AI firms, the NASA to 4 and the DoD to 3.

Big Tech control of the AI stack is extensive to its adoption milieu. From individual ChatGPT users to organizations purchasing products with an AI engine, such as facial recognition or speech to text services, they all run on the cloud. Most of the AI products do not have a stand-alone version that can be deployed locally and those that do, require infrastructure that only large organizations can afford. Amazon, Microsoft and Google, in that order, concentrate over 65% of the cloud computing market globally.[6] Besides profiting from the direct use of AI models, they offer -directly or through third-party companies that pay a fee to Big Tech- all sorts of complementary services, including but not limited to compute power for training, deploying and consuming AI.

How the whole AI stack works, depending on the cloud, profiting from academic and open source contributions and even how new firms produce AI, everything is part of a Big Tech corporate decision to lead and control AI. Google even complemented all these scattered pieces with a sort of AI Manhattan Project. In 2014, it acquired DeepMind, a frontier AI start-up. It then massively hired leading AI scientists and engineers turning DeepMind into an organization of hundreds of AI experts working in small teams for achieving technological breakthroughs. They got access to Google's data, digital infrastructure and already existing software solutions and worked with the vision of achieving artificial general intelligence in accordance with Google's priorities. DeepMind became a pioneering example of the industrialization of AI R&D that regularly funneled results to Google for developing products. Likewise, Microsoft has recently announced a project to create a centralized AI division for developing foundational models in connection with the start-ups that it is investing in and controlling.[7] In all, Big Tech companies plan AI.

[4] https://www.ft.com/content/c6b47d24-b435-4f41-b197-2d826cce9532

[5] Data comes from Crunchbase. A more detailed analysis is available at Rikap (2024b). "Dynamics of corporate governance beyond ownership in AI". Common Wealth.

[6] https://www.srgresearch.com/articles/q1-cloud-spending-grows-by-over-10-billion-from-2022-the-big-three-account-for-65-of-the-total

[7] https://blogs.microsoft.com/blog/2024/03/19/mustafa-suleyman-deepmind-and-inflection-co-founder-joins-microsoft-to-lead-copilot/

3. AI's dual-use applications or the business of disorder

AI is a dual-use technology, but Big Tech companies are not like other military contractors that developed military and commercial solutions side by side. The military industry is only one of many AI application verticals. Indeed, Amazon, Microsoft and Google offer a diversity of tailored military services on their clouds. For instance, Amazon Web Services (AWS) claims that its "shared security model is backed by more than 230 cloud security tools and services".[8] Nonetheless, this does not significantly differ from services for other sectors. From healthcare to retail, the cloud offers customized solutions for all. Business wise, military applications operate just like other industries. If anything, they are costlier because cloud providers need to comply with all the security requirements.

Yet, for the US NSS, AI and the cloud are indispensable. In its 2018 AI strategy, the US DoD (2018) advocated for harnessing AI as fundamental for advancing security and prosperity and warned that China and Russia are already making significant investments. The strategy also speaks of the cloud as a means to scale AI's impact across the DoD.

The US Defense Digital Services manages the US Air Force's control system of satellites in AWS GovCloud (US), an isolated AWS service that complies with all the US security requirements so that customers can "host sensitive Controlled Unclassified Information (CUI) and all types of regulated workloads".[9] And Microsoft's dedicate cloud solutions for the publica sector -Azure Government- includes generative AI services that are already being used by the US DoD and other agencies.[10]

Major US military providers also rely on Big Tech clouds for digital technologies. Lockheed Martin, Cobham Advanced Electronic Solutions, GDIT and Raytheon use AWS GovCloud. AWS claims that the latter has reduced the time to deploy test environments from four months to 15 days using AWS GovCloud (US).[11] In turn, Microsoft signed in late 2023 a strategic partnership agreement with Leidos, a tech companies specialized in AI for defense, to deliver AI to the US NSS.[12]

The cloud operates enabling to rent the use of computing services without real access to the technology; its use is sold as black boxes (Rikap & Lundvall, 2021). Thus, when the US NSS or any organization uses digital technologies on the cloud, it is significantly deprived from learning by doing, using and interacting with the technology. If the military does not understand how the technology works, the US NSS chances to autonomously define its strategy shrink and the dangers associated with using AI for military purposes expand.

The story of the US DoD and cloud computing is illustrative of the relevance of the cloud and the concern raised about Big Tech dominance. The Joint Enterprise Defense Infrastructure (JEDI) project was a US DoD cloud computing contract worth USD 10 billion. It was initially granted to Microsoft and then subjected to a new bid where Amazon and Microsoft were expected to share

---

[8] https://aws.amazon.com/government-education/worldwide/uk/national-security-and-defence/?wwps-cards.sort-by=item.additionalFields.sortDate&wwps-cards.sort-order=desc

[9] https://aws.amazon.com/govcloud-us/?whats-new-ess.sort-by=item.additionalFields.postDateTime&whats-new-ess.sort-order=desc

[10] https://www.bloomberg.com/news/articles/2023-06-07/microsoft-offers-powerful-openai-technology-to-us-government-cloud-customers?sref=z97LigUM

[11] https://aws.amazon.com/partners/success/raytheon/?did=psr_card&trk=psr_card

[12] https://www.forbes.com/sites/lorenthompson/2023/08/07/leidos-microsoft-partnership-is-latest-sign-ai-is-taking-the-defense-industry-by-storm/

the deal. By mid 2021, the US DoD replaced JEDI with the Joint Warfighting Cloud Capability (JWCC), which has a multi-vendor approach.[13] By December 2022, the US DoD had awarded JWCC contracts to AWS, Google, Microsoft and Oracle.

This multi-vendor strategy limits US cloud provider's capacity to impose conditions to the US DoD and allows the latter to remain in good terms with every US Big Tech. However, when it comes to overall contracts with the US DoD, this multi-vendor strategy gets more diluted. Microsoft, by afar, concentrates most of the sharp increase in the number and specially the monetary value of military (and security) procurement contracts. Between 2008 and 2021, Microsoft received USD 3.2 billion from the US DoD followed by Amazon, which was awarded USD 50 million (Coveri et al., 2023). These are meaningful figures but for Microsoft and Amazon they represent pocket money. Only in 2023, their respective total revenues were USD 211.91 billion and USD 574.8 billion.

Among the contracts that are not directly related to the cloud, the US Army has a major deal with Microsoft for HoloLens headsets, with plans to spend USD 21.9 billion on the project. This example highlights the US government internal tensions regarding relations with Big Tech. The US Congress rejected the Army request to fund 6.900 HoloLens goggles and also reduced the US Army funding request from USD 400 to USD 40 million that were given to Microsoft, with an additional USD 125 million coming straight from the US Army, for continuing the gadget's development.[14]

Featuring less prominently in the number and monetary value of awarded contracts (Coveri et al., 2023), Google's AI for military uses dates back, at least, to Project Maven. This was a Pentagon initiative that used Google's computer vision technologies to analyze drone surveillance footage. It came to light due to Google employees' protests, which led the company to allegedly withdraw from it. Recently, it came to light that Project Maven's AI was underpinning the US Military intensified use of AI tools since Hamas's terrorist attack and Israel's genocide in Gaza.[15]

In relation to Israel, Project Nimbus was a USD 1.2 billion cloud services contract of Google and Amazon[16] with the Israeli military and government that included the provision of technology "for facial detection, automated image categorization, object tracking, and even sentiment analysis that claims to assess the emotional content of pictures, speech, and writing".[17] This secretly kept project was disclosed by a group of Google and Amazon employees that denounced that Project Nimbus was, in fact, an Israeli army plan to use frontier AI for surveillance and unlawful data collection on Palestinians.[18]

---

[13] See: https://www.defense.gov/News/Releases/Release/Article/2682992/future-of-the-joint-enterprise-defense-infrastructure-cloud-contract/

[14] See: https://www.theverge.com/2023/9/13/23871859/us-army-microsoft-ivas-ar-goggles-success-new-contract-hololens

[15] On this specific issue see: https://www.bloomberg.com/news/articles/2024-02-26/us-says-it-used-ai-to-help-find-targets-it-hit-in-iraq-syria-and-yemen?utm_campaign=socialflow-organic&utm_content=tv&utm_medium=social&cmpid%3D=socialflow-twitter-tv&utm_source=twitter&sref=10lNAhZ9 and for a more comprehensive recount of Israel's massacres in Palestine and its use of AI for war see Wolfgang Streeck's (2024) piece in this special issue.

[16] Amazon was also accused of facilitating the expansion of Israel's illegal settlements in Palestine by supporting data for the Israel Land Authority (ILA) -which allocates and manages state land- technologies for analysing data https://www.thenation.com/article/economy/amazon-prime-day-israel/

[17] https://theintercept.com/2022/07/24/google-israel-artificial-intelligence-project-nimbus/

[18] https://www.theguardian.com/commentisfree/2021/oct/12/google-amazon-workers-condemn-project-nimbus-israeli-military-contract

Big Tech companies are also planning AI for military purposes beyond their own offered services and contracts. Their investments in AI start-ups are extensive to those focused on the military-industrial complex. Microsoft is among the main investors of Blackshark.ai, a start-up developing a military metaverse[19], and AWS launched a defense accelerator for start-ups working on specific focus areas aligned to AWS priorities.[20] Plexal, a United Kingdom Government supported innovation technology firm, worked with AWS to launch the 2023 AWS European Defence Accelerator.[21] Accelerators not only enable Amazon to copy or purchase those start-ups' technology but also promote AWS services' uptake, expanding the range of computing services that will afterwards be available on AWS's marketplace, thus reinforcing Amazon's cloud business (Rikap, 2023b). More generally, considering that the whole AI industry is being developed within Big Tech clouds, what Gonzales (2023) describes as the emergence of Silicon valley's digital defense industry can be seen as an extension of Big Tech's planned space.

Summing up, when compared to the Cold War period, governed interdependence in the development of frontier technology remains but the roles are inverted. In AI, it can be said that the US NSS is governed by a few private sector giants that do not depend on the former to make a business.

3.1. Planning US NSS priorities

Big Tech companies openly shape the US NSS transformation. In 2021, the US President and Congress asked an ad-hoc group dubbed the National Security Commission on Artificial Intelligence (NSCAI), chaired by the already mentioned Eric Schmidt and including top executives from Google, Microsoft and Amazon, to make recommendations for the development of AI and associated technologies aimed at addressing the US national security and defense needs. The NSCAI overall assessment is synthesized in the following quote:

> "(f)or the first time since World War II, America's technological predominance—the backbone of its economic and military power—is under threat. China possesses the might, talent, and ambition to surpass the United States as the world's leader in AI in the next decade if current trends do not change." (National Security Commission on Artificial Intelligence, 2021, p. 7)

Addressed to leaders in the Pentagon and Federal Government, the report argues that they must invest in AI R&D, particularly infrastructure, and suggests a reorganization of the US DoD and Intelligence Community to ensure that by 2025 they are AI-ready. In its 756 pages document, the NSCAI provides detailed instructions on how to do it. It is hardly likely that those corporate executives had the time to write almost 800 pages but their signatures as NSCAI members and authors of the report signal that they are instructing on how to transform the US NSS.

The report states that most AI R&D, while financed by the state, should be done by firms and universities. It also calls for more stringent IPRs for AI, data and biotechnology, arguing that insufficient protection has led inventors to prefer trade secrecy. This is a quite beneficial approach for Big Tech: while the US government makes colossal R&D investments, they retain and strengthen the means to collect associated gains.

---

[19] https://blackshark.ai/bisim-and-blackshark-ai-join-forces/

[20] https://aws.amazon.com/blogs/publicsector/announcing-first-aws-defence-accelerator-uk-startups/?did=psr_card&trk=psr_card

[21] https://www.plexal.com/our-work/aws-european-defence-accelerator/

In all, the NSCAI's report holds sway over in the US NSS. In 2023, under the light of the accelerated adoption of generative AI, both the head of the CIA and an FBI director emphasized the threat of being outpaced by China. This is why, according to the latter, the FBI is "proactively aligning resources to engage with the intelligence community and our private sector partners to better understand the technology and its downstream impacts."[22]

4. A frenemy relation

After decades of planning major technological breakthroughs, contemporary large-scale AI is not planned by the US NSS but by a handful of giant firms. This is a major source of instability in their relationship. US Big Tech companies plan AI for accumulation and corporate control which may not necessarily prioritize the development of AI for the US military domination. Clashes of power emerge due to the partial overlapping of their planning spheres and, ultimately, concern *who plans whom*.

The links between US Big Tech and Chinese organizations are a source of distress. Microsoft conducts R&D in China since 1998 in close collaborations with universities and companies, including Chinese Big Tech. Between 2012 and 2021, 24% of Microsoft's total publications had at least one author based in China. From the 120 countries represented in its publications, only the US appeared more than China.

Because the development of AI for military uses cannot be detached from commercial and foundational AI, Microsoft research in China contributes to China's military AI even when it is not directly aimed at developing military applications simply by enhancing the AI capabilities of Chinese organizations as they co-create knowledge. In line with its strong foothold in China's innovation landscape, a dozen Chinese AI firms declared having Microsoft among their top funders by February 2024, representing 24% of all the AI firms with Microsoft as a top investor. By the same date, Google was featured among the top funders of the Chinese company Mobvoi, also known as Chumenwenwen, which develops technologies in Chinese language for speech recognition and natural language processing. Microsoft also partnered with the National University of Defense Technology, an institution controlled by the Central Military Commission of the People's Republic of China, for AI research (Rikap, 2024a).

The US NSS and broadly the US state interest in bargaining with -and eventually taming- Big Tech could be even larger than what I have portrayed so far considering that asymmetric global networks controlled by multinational corporations can be used by those companies' home states as weaponized networks. A state can coerce other states by leveraging on its companies if the latter control chokepoints and/or enjoy a panopticon view of the whole network. This is what Farrell and Newman (2019) conceptualized as weaponized interdependence. US Big Tech control of digital infrastructure (Gjesvik, 2022), the whole global AI innovation system and digital platforms of all types can be seen as cases in point that further expand the US state inclination to have a friendlier approach to Big Tech for the weaponization of these networks.

At the other end the relation, I have already argued that US Big Tech companies do not depend on public funding and their military business is negligible in comparison to the size of their overall operations. Nonetheless, they rely on their home state's capacity to keep Chinese rivals at bay and

[22] See https://cyberscoop.com/fbi-officials-cybersecurity-china-ai/ and https://www.globalgovernmentforum.com/we-have-to-do-it-faster-and-better-than-they-do-cia-chief-sets-out-era-of-us-china-strategic-competition-in-ai-and-beyond/

for limiting regulations that constraint their businesses in the rest of the world. The latter is pretty much what the US state did when France proposed taxing Big Tech revenues.

This tit-for-tat could be seen as the unfolding of what Strange (1992, p. 7) termed corporate-state diplomacy. With the spread and growth of multinational corporations, she explained, governments had to bargain with them as much as with other governments. This is because, continues the author, transnational corporations command "an arsenal of economic weapons that are badly needed by any state wishing to win world market shares" among which technology looms large. Building on her work, Babic et al. (2017) argue that states and corporations are not subordinated to each other but juxtaposed and intertwined; they use each other to increase their respective power positions. In the same vein, when speaking of power relations, Arrighi (2009, p. 150) takes from Talcott Parsons the distinction between distributive power as a zero-sum game and collective power as a positive-sum-game and argues that the latter is exercised when "cooperation among distinct agencies increases their power over third parties or over nature".

Although these ideas are insightful and can be mobilized as starting points for analyzing corporate and political powers interplay more broadly, in the case of AI, this mutual dependency is unbalanced. This is why I suggest speaking of frenemies, which denotes a relation that even if can be favorable to both parties, is not among equals. The US NSS is prone to be a Big Tech frenemy because American primacy depends crucially -even more as times become more turbulent- on their AI intellectual monopolies. On the contrary, as much as Big Tech need to keep rivals and regulators at bay, unlike the US NSS with AI, they do have other means -such as direct lobby- to achieve these goals.

4.1. Strategic allies amid mounting conflicts

The current turbulent times will likely reinforce the use of AI as guarantor of the US primacy. The NSS is already increasing its AI uptake[23] and, considering the sense of military urgency that usually comes with conflict escalation[24], Western states will probably deepen their entanglement and dependence on US Big Tech companies. In such a scenario, considerations about the implications of using AI for surveillance and military purposes may be left for aftermath discussions, which would further favor Big Tech and the US NSS.

Contemporary disorder also offers US Big Tech more space to plan AI, shaping regulations and narratives, entrenching their AI dominance globally beyond the military-industrial complex. The US AI regulation should be understood within this context. As the US vice-president Kamala Harris stated when the US Executive AI Order "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" was released:

> "Let us be clear: when it comes to AI, America is a global leader. It is American companies that lead the world in AI innovation. It is America that can catalyse global action and build global consensus in a way that no other country can."

[23] See https://www.bloomberg.com/news/articles/2024-02-26/us-says-it-used-ai-to-help-find-targets-it-hit-in-iraq-syria-and-yemen?utm_campaign=socialflow-organic&utm_content=tv&utm_medium=social&cmpid%3D=socialflow-twitter-tv&utm_source=twitter&sref=10lNAhZ9 and https://www.forbes.com/sites/lorenthompson/2023/08/07/leidos-microsoft-partnership-is-latest-sign-ai-is-taking-the-defense-industry-by-storm/

[24] For instance, the European Union has already called to subsidize the defense industry https://www.ft.com/content/66606e2c-0b5a-493e-af59-d24436d0fd72?segmentId=b0d7e653-3467-12ab-c0f0-77e4424cdb4c

This executive order does not mandate to disclose what data was used for training or the model parameters. It mainly regulates harmful AI uses. And this is precisely what Big Tech wanted. Months ahead of the regulation, at an interview for CNBC on May 16th, 2023, Microsoft's CEO Satya Nadella had made an open case for regulating AI applications, remaining silent about the regulation of AI production where Microsoft looms large, as this piece has highlighted:

> "We do not have to wait for regulation to have standards or adopt the misstandard, I call it the start of any self regulation. Then, on top of that, if we talk about regulation, maybe we can unpack it from the application domain, because after all context in which something is being applied, in education, healthcare, retail and we can have the regulatory frameworks that already exist."

The US AI regulation is a peace offering that speaks of the US NSS dependence on Big Tech. It arrived as the US Federal Trade Commission (FTC) was decisively moving against them. During Biden's administration, the US FTC was occupied by Neo-Brandeisians seeking to transform -by expanding- what is considered as market power abuses. They counted on their side a growing civil society and academic consensus critical of Big Tech. The resulting internal tension of the US federal government can be conceived as a swing, with episodes in which the US FTC leads the offensive against Big Tech and episodes in which the US NSS's need for AI reinforces US Big Tech companies' intellectual monopolies.

As the US FTC moves forward, the US NSS reacts. In 2021, 12 former US national security officers signed a letter against antitrust using the same argument of Big Tech during the US Congress Hearing of 2020: regulation stifles innovation undermining the US in its race against China.[25] Underlying this argument, one must remember that most of the innovation is actually produced by or co-produced with organizations that barely profit from it (Rikap, 2023a, 2023b; Rikap & Lundvall, 2021) and that not every innovation is beneficial for society. Unsurprisingly, the 12 former national security officials had ties with Big Tech.[26]

In sum, as global turbulence intensifies, it is in the best interest of the US NSS to secure frontier AI for the military-industrial complex which, all things considered, implies accepting that this technology is planned by US Big Tech. As long as regulations favor decoupling US Big Tech AI from China and the discontent due to Big Tech's escalating power is ward off, being governed by these giants is a relatively low price to pay for the US NSS's purposes. In the end, American primacy would still be realized. In such a scenario, both the US NSS and Big Tech could reinforce their respective exercise of power and accumulate at the expense of the rest of the world.

5. The space for building an alternative

This piece has sketched the interplay between the US NSS and Big Tech, which are among the world's most powerful actors, as a frenemy relation. By advancing AI, a general-purpose technology with diverse applications for surveillance and military uses, US Big Tech companies reinforce American primacy. Concerns related to these giants' AI planning -who they develop AI with and how- were not at the expense of the US NSS push for introducing their technologies wide and large. In fact, the US DoD recognizes the need to partner with AI leaders (see for instance US

[25] https://www.axios.com/2021/09/15/china-antitrust-big-tech-national-security
[26] https://www.politico.com/news/2021/09/22/former-security-officials-antitrust-tech-ties-513657

Department of Defense, 2018, 2023). Commissioning the NSCAI to Big Tech gives further testimony of the latter and not the US NSS planning AI.

By identifying that Big Tech are planning today's cutting-edge technology, an underlying finding of this piece is that, unlike what many assert (see for instance Ruttan, 2006; Schmidt, 2023), the military-industrial complex is not indispensable for major technological change. Contemporary AI, controlled by Big Tech and associated with the expansion of big data that sprang from digital platforms, was not planned by the US NSS. Yet, if there is one thing that remains, is that major technological change is still planned. The Manhattan Project, the US NSS during the Cold War and how Big Tech companies develop and control AI are all examples of successful innovation planning.

Planning requires clearly defining in advance the purpose and urgency as well as a strategy that serves as a roadmap that is anyway subject to adaptations as investigations progress. For Big Tech, the purpose is profits and the reinforcement of their intellectual monopolies, which is achieved by planning the whole AI stack. For the US NSS, this is safeguarding American primacy. Planning innovation includes defining priorities and identifying the institutions -existing ones and to be created-, the organizations and individuals that can most likely deliver. DARPA and how Google built DeepMind as a moonshot division are prominent examples of such institutions. Microsoft, as I have mentioned, is creating its own CERN-like AI center.

Securing necessary investments is essential for planning innovation. Investment -as Durand and Keucheyan (2024) explain for the case of ecological planning- is a planning instrument. The US NSS used public procurement and funded R&D internally and in other organizations. Big Tech companies also do the latter and massively use venture capital for planning AI. Likewise, the US NSS invests in start-ups, but this instrument is marginally used in comparison to Big Tech.

Big Tech's AI planning has resulted in innovations that, to say the least, are not primarily seeking to solve major social and ecological hardships. The scenario is even bleaker in China where the state openly provides citizens' data to AI companies for the development of technologies that are extremely entangled with military and surveillance applications. The decisions of what science and technology is needed can neither be left in the hands of the defense and military apparatus nor at the mercy of corporate giants.

By recognizing that planning is indispensable for achieving major technological breakthroughs, we open a space for building an alternative: the democratic planning of science and technology, notably AI, at the service of addressing current social and environmental breakdowns. Such an ambitious project calls for the revival of development banks or similar institutions, now empowered with digital technologies to foresee and steer the economy. This shall be addressed together with macroeconomic coordination or planning, among which the space for monetary policy looms large (Brancaccio et al., 2024).

The stakes are high because of past failed experiences of planning without democracy. The emphasis on democracy for planning stresses the political nature of every plan. It simultaneously distinguishes this proposal from both failed socialist attempts and Big Tech and military planning. Plans designed by experts that -choose to- ignore the social, political, economic and environmental implications of science and technology cannot be seen as democratic either. Drawing on Durand and Keucheyan (2024), workers must partake in deciding priorities and the organization of labour and this shall be extensive to the organization of science and technology.

Democratic AI planning would require creating new institutions beyond investment banks that give voice and decision-making power to those that today co-produce AI in silence, from AI micro-workers (Cardon & Casilli, 2015) to AI scientists critical of their field. Given the direct impact of AI in the workplace, unions must participate as well as scholars, civil society organizations and grassroots movements with expertise in AI's various -potentially harmful or unequal- effects or implications. AI is precisely a technology that could be mobilized for the constant democratic reassessment and adjustment of plans, gaining in flexibility without losing sight of collectively agreed aims of AI for peace. These, instead of prioritizing profits or military supremacy, shall put people and the planet first.

This project will inevitably face confrontations with those that today concentrate income and wealth as they see the scale tilting against their interests. To counterbalance these pressures, wide citizens' support is fundamental. More research is needed on existing experiences and ways to create new architectures for democratic planning based on building new common senses that do not associate every form of planning with the absence of democracy.

Anyway, none of these proposals are silver bullets. I see all the above as building blocks of a comprehensive plan to restructure the global economy to create a world in which freedom is not an individual prerogative of a few. Freedom shall be a collective search that springs from building democratic institutions for the present and for planning the future. Such a project is unfeasible today. The job is therefore to put the collective intellect of the majorities, of those from below, at the service of designing concrete solutions that complemented with the democratic planning of science and technology could orchestrate a future for all where human life is co-produced in harmony with other species and nature.

6. References

Arrighi, G. (2009). *Adam Smith in Beijing: Lineages of the 21st century*. Verso books.

Babic, M., Fichtner, J., & Heemskerk, E. M. (2017). States versus corporations: Rethinking the power of business in international politics. *The International Spectator*, *52*(4), 20–43.

Baines, J., & Hager, S. B. (2023). *Rentiership and Intellectual Monopoly in Contemporary Capitalism: Conceptual Challenges and Empirical Possibilities*.

Block, F. (2008). Swimming against the current: The rise of a hidden developmental state in the United States. *Politics & Society*, *36*(2), 169–206.

Boldrin, M., & Levine, D. K. (2004). 2003 Lawrence R. Klein Lecture The Case Against Intellectual Monopoly. *International Economic Review*, *45*(2), 327–350.

Brancaccio, E., Giammetti, R., & Lucarelli, S. (2024). Centralization of capital and "economic conditions for peace". *Review of Keynesian Economics*. 12(3), 365-384

Cardon, D., & Casilli, A. (2015). *Qu'est-ce que le digital labor?* Ina.

Coveri, A., Cozza, C., & Guarascio, D. (2023). *Blurring boundaries: An analysis of the digital platforms-military nexus*. GLO Discussion Paper.

Durand, C., & Keucheyan, R. (2024). *Comment bifurquer—Les principes de la planification écologique* (La Decouverte).

Durand, C., & Milberg, W. (2020). Intellectual monopoly in global value chains. *Review of International Political Economy*, *27*(2), 404–429. https://doi.org/10.1080/09692290.2019.1660703

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, *44*(1), 42–79.

Gjesvik, L. (2022). Private infrastructure in weaponized interdependence. *Review of International Political Economy*, *30*(2), 1–25.

Gonzales, R. (2023). Militarising big tech. The rise of silicon valley's digital defence industry. *TNI, Available at: Https://Www. Tni. Org/En/Article/Militarising-Big-Tech*, 1–12.

Mandel, E. (1986). In defence of socialist planning. *New Left Review*, *159*(1), 5–22.

Mazzucato, M. (2013). *The entrepreneurial state: Debunking public vs. private sector myths* (Vol. 1). Anthem Press.

Miller, C. (2022). *Chip War: The Fight for the World's Most Critical Technology*. Simon and Schuster.

National Security Commission on Artificial Intelligence. (2021). *Final Report*.

Pagano, U. (2014). The crisis of intellectual monopoly capitalism. *Cambridge Journal of Economics*, *38*(6), 1409–1429.

Phillips, L., & Rozworski, M. (2019). *The People's Republic of Wal-Mart: How the World's Biggest Corporations Are Laying the Foundation for Socialism*. Verso.

Rabinovich, J. (2023). Tangible and intangible investments and sales growth of US firms. *Structural Change and Economic Dynamics*, *66*, 200–212.

Rikap, C. (2021). *Capitalism, Power and Innovation. Intellectual Monopoly Capitalism uncovered*. Routledge.

Rikap, C. (2023a). Capitalism as Usual? Implications of Digital Intellectual Monopolies. *New Left Review*, *139*(Jan), 145–160.

Rikap, C. (2023b). Intellectual monopolies as a new pattern of innovation and technological regime. *Industrial and Corporate Change*. https://academic.oup.com/icc/advance-article-abstract/doi/10.1093/icc/dtad077/7462137

Rikap, C. (2024a), '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, doi: https://doi.org/10.1080/09692290.2024.2365757*

Rikap, C. (2024b), 'Dynamics of corporate governance beyond ownership in AI', Common Wealth. Available at: https://www.common-wealth.org/publications/dynamics-of-corporate-governance-beyond-ownership-in-ai

Rikap, C., & Lundvall, B.-Å. (2021). *The Digital Innovation Race: Conceptualizing the Emerging New World Order*. Palgrave Macmillan.

Ruttan, V. W. (2006). *Is war necessary for economic growth?: Military procurement and technology development*. Oxford University Press.

Schmidt, E. (2023). Innovation power: Why technology will define the future of geopolitics. *Foreign Aff.*, *102*, 38.

Skidelsky, R. (2024). The Political Economy of War and Peace. *Review of Keynesian Economics*.

Strange, S. (1992). States, firms and diplomacy. *International Affairs*, *68*(1), 1–15.

Streeck, W. (2024). Notes on the Political Economy of War. *Review of Keynesian Economics*. 12(3), 293-307.

US Department of Defense. (2018). *SUMMARY OF THE 2018 DEPARTMENT OF DEFENSE ARTIFICIAL INTELLIGENCE STRATEGY Harnessing AI to Advance Our Security and Prosperity*. US Department of Defense.

US Department of Defense. (2023). *Data, Analytics, and Artificial Intelligence Adoption Strategy. Accelerating Decision Advantage*. US Department of Defense.

Wade, R. H. (2017). The American paradox: Ideology of free markets and the hidden practice of directional thrust. *Cambridge Journal of Economics*, *41*(3), 859–880.

Weiss, L. (2014). *America Inc.?: Innovation and enterprise in the national security state*. Cornell University Press.