

Blurring boundaries: AI and the military-digital complex

Dario Guarascio¹

¹Sapienza University of Rome

12 August 2025

ISODARCO - 63^d EDITION

Outline

What is behind the AI's hype?

Enters the military-digital complex

The military-digital complex reshapes industrial and innovation policy

AI at the core of contemporary warfare

Discussion: challenges for the governance of AI

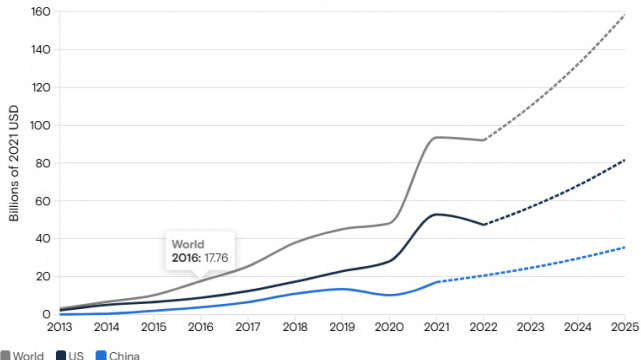
Davos 2024: 'the future of AI is the future of humanity'



An AI (financial) bubble?

AI investment is likely to grow in the next three years

Private AI investment (dotted lines show GS revenue projections*)



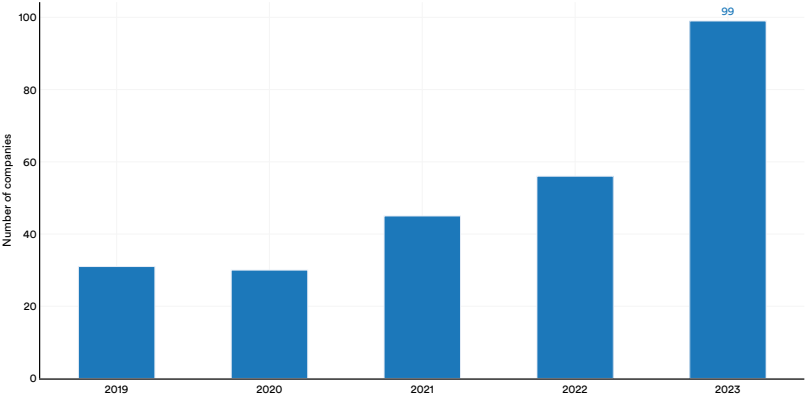
Source: Stanford Institute for Human-Centered Artificial Intelligence, Goldman Sachs Research
*Average of GS Research 2022-2030 revenue growth estimates for Microsoft Azure, NVIDIA, Google Cloud, and Amazon Web Services (when available)

**Goldman
Sachs**

New AI ventures (2015-2024)

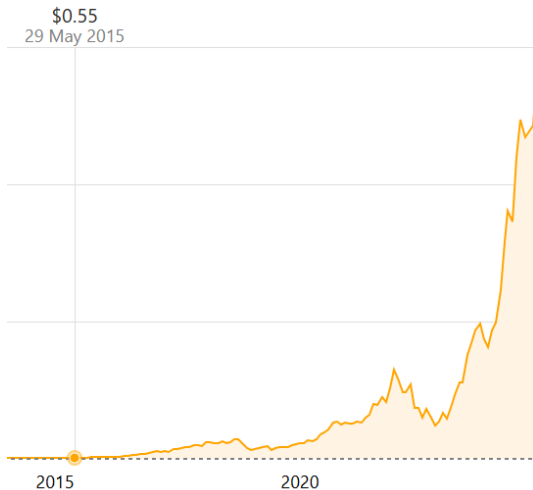
Number of newly funded generative AI companies in the world, 2019–23

Source: Quid, 2023 | Chart: 2024 AI Index report



Microchips (GPUs) matter...

Nvidia stock price history (2015-2024)



What is behind the AI's hype?

- ▶ Hyping around new technologies as a way to 'depoliticize' the debate? Industry leaders trying to hegemonize the discussion, AI framed as a neutral shock and policies only as a way to properly adjust/regulate, financial bubbles
- ▶ What's going on behind the AI hype? AI further strengthening the power of Big Tech, reinforcing winner-takes-all mechanisms (e.g., the cloud industry), restructuring of VCs (e.g., Nvidia) and exacerbating geopolitical conflicts, deepening labour fragmentation plus digital colonialism, the military-digital complex...

Digital technologies and AI: civilian vs military trajectories

- ▶ From the early stages of the **ICT technological paradigm** (Dosi, 1982) to the recent AI's discontinuity → Is it a new technology? A GPT?
- ▶ **The complex interplay** between civilian (market driven, cost minimisation, mass consumption, competition among oligopolists building on a variety of capabilities) and military (missions, command and control, maximum performance requirements, frequent economic inefficiencies) goals shaping the ICT technological trajectory (Guarascio and Pianta, 2025)
- ▶ **Key interaction between market relations and political agency on an international scale** → changing division of labour and techno-economic hierarchies, winners and losers in both the economic and the geo-political/military domains

A disturbing convergence:

Big Tech monopolistic goals and the 'digitalization of war'

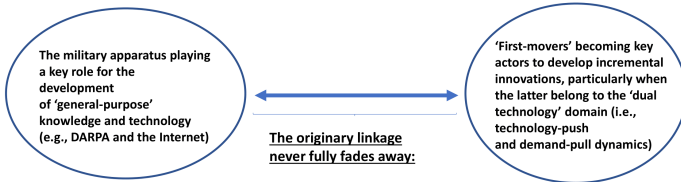
- ▶ Iraq, Afghanistan, local wars, cyberwars, US-China rivalry: the role of digital technologies becomes paramount in military strategies, both as a factor shaping global technological hierarchies and as a key component of frontier weapon systems
- ▶ Military priorities and procurement contracts becoming a rapidly growing area of activity of Big Tech, with potentially relevant impacts on the evolution of the ICT paradigm
- ▶ Emphasis on surveillance, remote-control and autonomous systems, manipulation of information and social control may affect the evolution of applications in commercial and public service domains → relevant policy implications (public priorities, balance of power between military and civilian interests)

Disentangling the military-digital complex (1)

- ★ The ‘originary linkage’ binding military apparatus and digital platforms:
- ▶ Big Tech owe their emergence to military projects (i.e., DARPA) supporting the development of **basic knowledge and technologies** and, no less importantly, favouring **technology transfer** (Mowery, 2010; O’Mara, 2020).
- ▶ A ‘pendulum-like’ relationship: the originary linkage never fades away completely, even when corporate R&D become mostly oriented towards private demand and civilian purposes → military apparatuses continue to have an active role, affecting the evolutionary trajectory of products and technologies via, for example, military patents (Schmid, 2018)...institutions and procedures working as an ‘always-open backdoor’ for military apparatuses to monitor and, if needed, affect corporations’ strategies are systematically established.

Disentangling the military-digital complex (2)

The 'pendulum-like' relationship



- Public R&D is needed to achieve radical breakthroughs
- 'Backdoors' to encourage convergence of strategies when strategic needs emerge
- Military patents

Disentangling the military-digital complex (3)

★ Knowledge, technology and critical infrastructures:

- ▶ **Big Tech monopolize key assets** (e.g., cloud, submarine cables), hold the majoritarian share of digital patents (Fanti et al., 2022) and are the loci where most of the formal and tacit knowledge is developed (Rikap et al., 2021)
- ▶ **Military operations** involving the creation of a new surveillance system, access to sensitive information, protection from a cyberattack, deployment of a satellite system in remote, high-risk areas can hardly be realised without the cooperation of platforms
- ▶ Big Tech **idiosyncratic competencies** are key given their tacit and cumulative nature → as digital infrastructures grow in terms of size and relevance (e.g., increasing the mass of information stored and processed), the efficiency of embedded technologies (e.g., machine learning (ML) algorithms) and the uniqueness ('black-boxishness') of corporation-specific competencies increase too...

Disentangling the military-digital complex (4)

- ▶ Pivotal role in both **civilian and military innovation ecosystems** (Jacobides et al., 2024) → governing knowledge co-creation processes and exploiting the modular structure of digital ecosystems, benefiting from the decentralized nature of digital innovation while preserving their economic and technological power.
- ▶ **Attracting top skills:** in frontier fields such as Big Data, AI, or Quantum Computing Big Tech have a significant competitive advantage → career prospects and incomparable economic levers (e.g., stellar salaries and stock options)

Disentangling the military-digital complex (5)

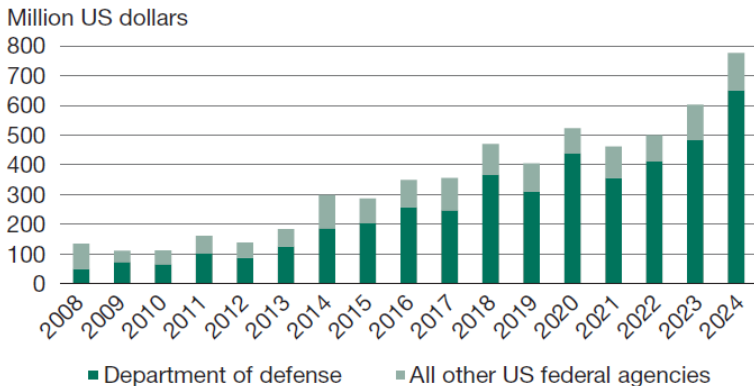
★ Digital platforms as ‘eyes and ears’ of governments:

- ▶ **At home**, Big Tech are a relevant ‘arm’ of their government’s security, intelligence and law enforcement → e.g., Microsoft has repeatedly shared threat assessments and reports of cyberattacks with the US government, while Facebook and Twitter have intervened to stop ‘disinformation’ campaigns by taking down networks of hijacked computer devices
- ▶ **Abroad**, Big Tech become ‘eyes and ears’ of their home state intelligence and military apparatuses: i) by partnering with platforms governments strengthen their grip on economies belonging to their ‘sphere of influence’ ii) gain advantage over enemies iii) enact what Kwet (2019) calls ‘digital colonialism’, *"Assimilation into the tech products, models, and ideologies of foreign powers – led by the United States – constitutes a twenty-first century form of colonisation"*

The military-digital complex

Big Tech's procurement contracts

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



The military-digital complex

Big Tech multi-year military and security contracts

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

Year and Department/ Agency	Contractor	Value (\$)	Nature of service	Declared aim
2013 — CIA	Amazon	600 million	Cloud	Data management aimed at preventing terrorist attacks
2019 — DoD	Alphabet (withdrawn); Amazon and Microsoft	50 million	Drones	Acquisition of AI technologies to improve image recognition in military drones ('Project Maven')
2020 — CIA	Alphabet, Amazon, Microsoft and Oracle	Tens of billions ²³	Cloud	Cloud services centralised for 17 intelligence agencies (Commercial Cloud Enterprise)
2021 — DoD	Microsoft	21.9 billion	Augmented reality visors	'HoloLens augmented reality headset' for military activities in highly complex contexts
2022 — NSA	Amazon	10 billion	Cloud	Cloud infrastructures for NSA ('Wild and Stormy' project)
2022 — DoD	Microsoft	NA	Stryker armoured vehicles	Digital devices to be incorporated into armed vehicles
2022 — DoD	Alphabet (Google public sector division)	NA	Google workspace	Provision of Google Workspace to 250,000 DoD employees
2022 — DoD	Alphabet, Amazon, Microsoft and Oracle	9 billion	Cloud	Cloud infrastructure for the 'Joint Warfighting Cloud Capability' (JWCC)
2022 — DoD	Amazon and Microsoft	NA	Satellites	Space- and ground-based infrastructure for national security ('Hybrid Space Architecture' program)
2022 — DoN/DoD	Amazon	724 million	Cloud	Cloud services to process and store data for critical missions
2023 — SSC/DoD	Microsoft	19.8 million	Cloud-based space simulation (viewable with Microsoft HoloLens headsets)	Space simulator aimed at gaining situational awareness and acting faster than adversaries
2024 — DoD	Amazon	22 million	Cloud	Cloud services for the Army department of the US Special Operations Command

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

The military-digital complex reshapes industrial and innovation policy (1)



The military-digital complex reshapes industrial and innovation policy (2)

- ▶ **The digitalization of the defense budget:** US government expenditure in digital-related military technologies – including R&D, arms procurement and systems management – is skyrocketing, now in the range of about \$100 billion (2024) → AI, 5G, quantum sciences, cyberwars, hypersonics, autonomous weapons and space
- ▶ **DARPA's changing strategy:** after 2001 focus shifting on dual-use digital technologies and transfer from commercial to military applications (Fuchs, 2010, Guarascio & Pianta, 2025)
- ▶ **The Defense Innovation Unit:** liaison from DoD and warfighter needs to Silicon Valley (Harper, 2020) → operating like a commercial venture, entering into transaction agreements with private firms circumventing DoD's bureaucratic procedures process

The military-Big Tech ‘revolving doors’

- ▶ **Revolving doors:** i) imperative for governments to leverage knowledge and networks maintained by former executives to advance cutting-edge technologies for military-related initiatives ii) their experience and linkages make former members of the military apparatus key assets for digital corporations
- ▶ **Relevant cases, examples:**
 - ✓ **Former Apple vice-president (Doug Beck)** appointed as the new director of the Defence Innovation Unit (DIU)
 - ✓ **Former Alphabet CEO (Eric Schmidt)** member of the Defense Innovation Advisory (DIA) and the National Security Commission on AI (NSCAI)
 - ✓ **Former executive director of the Defense Innovation Advisory (DIA) (Josh Marcuse)** becoming head of strategy and innovation for Google Public Sector
 - ✓ **Retired US General Keith Alexander** former director of the National Security Agency (NSA) assumed a position on Amazon’s Board of Directors

Big Tech go to war: the Ukrainian battlefield (1)

- ▶ **Apple:** took the field by blocking Apple Pay electronic payments and stopping sales of its products in Russia
- ▶ **Alphabet:** banned access to advertising and distribution of Russian state media and increased security measures for user access in Ukraine
- ▶ **Facebook and Youtube:** block Russian contents and state media channels RT and Sputnik from their platform
- ▶ **Amazon:** stopped allowing new sign-ups for AWS in Russia and Belarus; Ukrainian government and PrivatBank (largest Ukrainian private bank) transferred most of their critical public and private data to AWS and are currently operating through this cloud
- ▶ **Microsoft:** announced about \$100 million in additional technology aid for Ukraine through 2023, bringing its total support for Ukraine to over \$400 million since the war began

Big Tech go to war: the Ukrainian battlefield (2)



[Who We Are](#) [What We Do](#) [Our Workplace](#) [Our Impact](#) [Our Planet](#) | [Follow Us](#) [Subscribe](#) [EN](#)

[News](#) / [AWS](#)

4 min

June 9, 2022

[f](#) [t](#) [in](#) [e](#) [s](#)

Safeguarding Ukraine's data to preserve its present and build its future

Written by Amazon Staff



AI at the core of contemporary warfare: The Lavender system

≡ **+972**
MAGAZINE

✉ Newsletter



SUPPORT US

‘Lavender’: The AI machine directing Israel’s bombing spree in Gaza

The Israeli army has marked tens of thousands of Gazans as suspects for assassination, using an AI targeting system with little human oversight and a permissive policy for casualties, +972 and Local Call reveal.

AI at the core of contemporary warfare: The US DoD's AI strategy



Why AI is so crucial for the military?

► Decision-making (DoD, 2024):

- ✓ Battlespace awareness and understanding
- ✓ Adaptive force planning and application
- ✓ Fast, precise, and resilient kill chains
- ✓ Resilient sustainment support
- ✓ Efficient enterprise business operations

► Autonomous weapons (Karpinsky, 2024):

- ✓ Drones, robots
- ✓ AI-enhanced traditional weaponry

► Surveillance, space and cyber-wars (Coveri et al., 2024):

- ✓ New generation satellites and surveillance technologies
- ✓ Pursuing and preventing cyberattacks

The Palantir's AI Platform or Defense

The screenshot displays the Palantir AIP (Artificial Intelligence Platform) interface, which is designed for defense operations. The interface is divided into several sections:

- Left Sidebar:** Contains the Palantir logo and the text "INTRODUCING AIP FOR DEFENSE".
- Top Bar:** Features a green header with "UNCLASSIFIED NOTIONAL DATA" and navigation tabs for "AIP Terminal", "Investigations", and "Proposals".
- Main Content Area:**
 - Alert Section:** Displays an alert titled "Alert - Anomalous military activity detected" with a timestamp of "20 April 2023 14:39Z". It includes a "Show me more details" button and a "Hand-off Inspector" link.
 - SAR Imagery:** A satellite image showing a terrain with several orange markers indicating detected military equipment.
 - Summary:** A text box stating: "This satellite image was captured 8 minutes ago. An algorithm that detects military equipment found 5 pieces of equipment in the image."
 - Details:** A table of metadata:

Details	Value
Timestamp	20 April 2023 14:39Z
Satellite	StarTech N-56200
Imagery Type	SAR
Image Quality	1m
Algorithm	Military Vehicle Detector V 25.3.0
- Right Panel:** A "Battlefield Overview" map showing a large red-dashed "Alert Region". Key locations marked include "Military Command", "Control Facility", "Alert Region", "15th Artillery BN", "Team Foxtrot", "72nd Armor Brigade", "Power Plant", and "Team Omega".
- Bottom Bar:** Includes a search bar with the text "What military unit is in the region?" and a "Start typing something to explore with AIP..." prompt.

AI & the military-digital complex:

Where are we?

- ▶ AI technologies playing a pivotal role in contemporary warfare (e.g., autonomous weapons, drones, cyberattacks and surveillance) → increasing the [State-Big Tech mutual dependency](#) (see ‘Blurring boundaries’, Coveri, Cozza & Guarascio, 2024)
- ▶ As development (and management) of AI technologies is strongly related to [infrastructure and capabilities concentrated in the hands of a few corporations](#), this can increase their power vis-à-vis the state with relevant implications also from a geopolitical point of view (e.g., Starlink in the Russia-Ukraine war, Google providing AI-based technologies to the IDF)

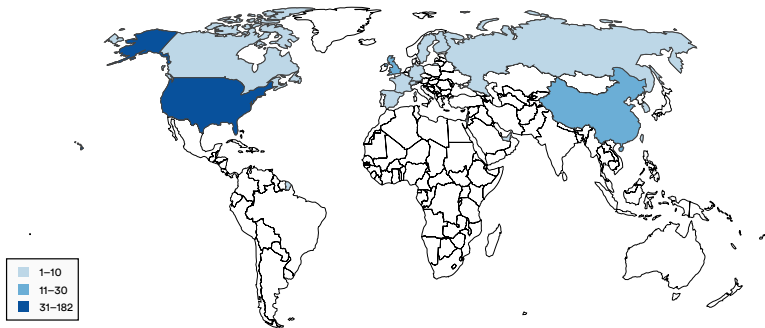
AI and the military-digital complex: Big Tech, but bigger (O'Mara, 2024)?

- ▶ **Big Tech** are practically the only entities with the superabundance of data, computing power, and funds required to make advanced AI possible (Coveri et al., 2022, 2024)
- ▶ **Leading foundational AI models** have come either from Big Tech-funded firms – e.g., OpenAI receiving a \$10 billion investment from Microsoft and Anthropic, \$4 billion from Amazon – or from Big Tech themselves
- ▶ **Relevant discontinuities with respect to the early stages of the Internet (1990s):** key corporations dominating R&D and patents, controlling relevant infrastructures, participating in the regulatory conversation, meeting heads of state, and explaining their bafflingly complex technology (in their own terms) to the world

Who owns the foundational models? (1)

Number of foundation models by geographic area, 2019–23 (sum)

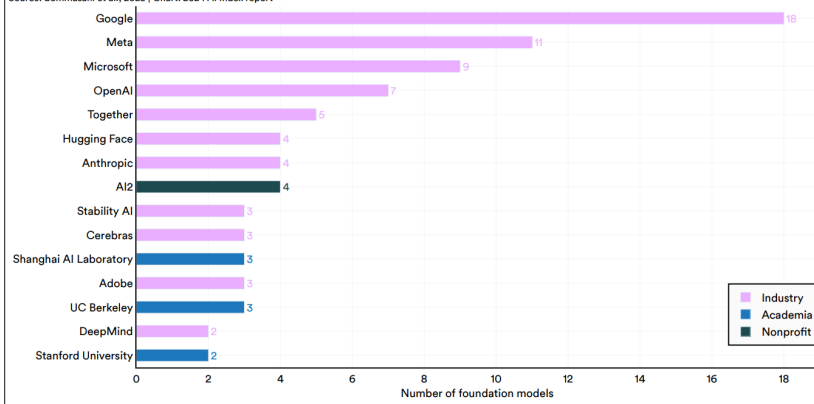
Source: Bommasani et al., 2023 | Chart: 2024 AI Index report



Who owns the foundational models? (2)

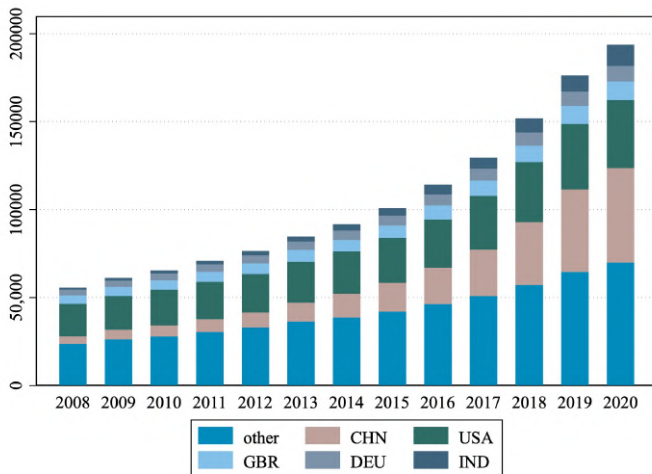
Number of foundation models by organization, 2023

Source: Bommasani et al., 2023 | Chart: 2024 AI Index report



Who controls AI-related knowledge and technology?

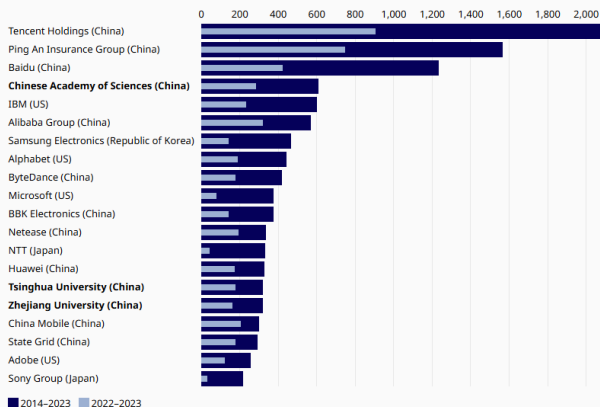
Top cited AI publications (Source: OECD)



Who controls AI-related knowledge and technology?

Top patent owners (Source: WIPO)

Figure 12 Top patent owners in GenAI, 2014–2023

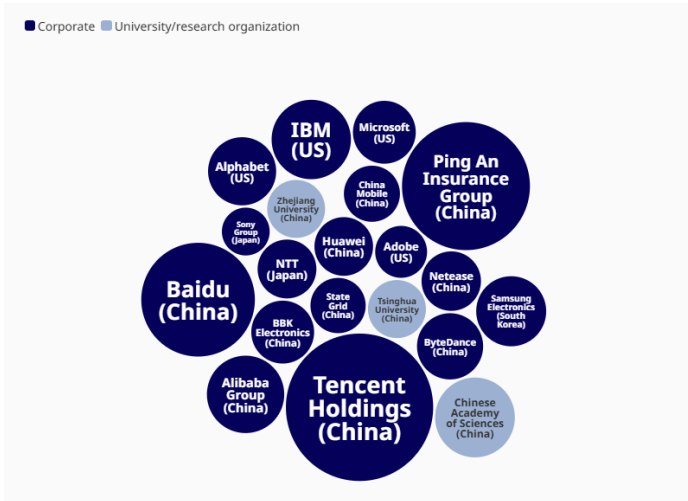


Note: Published patent families in GenAI.

Source: WIPO, based on patent data from EconSight/IFI Claims, April 2024. • [Get the data](#)

Who controls AI-related knowledge and technology?

Top patent owners (Source: WIPO)



Firm-level competition as the solution?

Not really...

THE WALL STREET JOURNAL.

English Edition • Print Edition • Video • Audio • Live Newsroom • More »

Subscribe Sign In

US ELECTION SALE

Latest World Business U.S. Politics Economy Tech Markets & Finance Opinion Arts Lifestyle Real Estate Personal Finance Health Style Sports



Struggling AI Startups Look for a Bailout From Big Tech

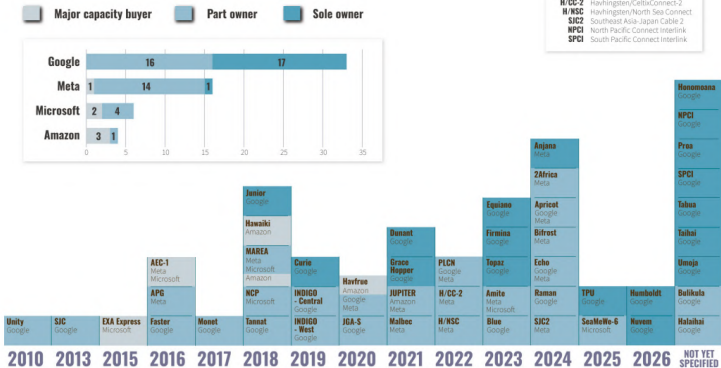
Amazon, Google and Microsoft are using a new type of deal to get employees and technology from artificial-intelligence firms



Power concentration in the AI ecosystem: Submarine cables (Source: Telegeography)

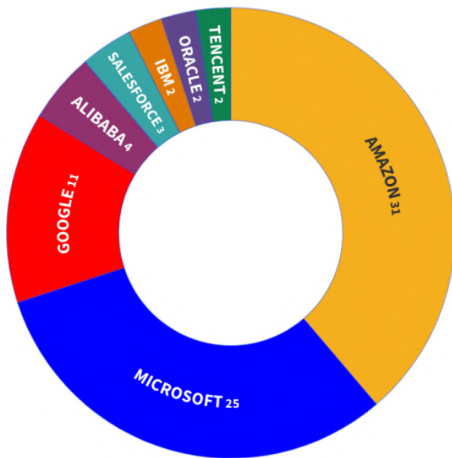
Hyperscaler investment in cables

The graph below illustrates the publicly disclosed submarine cable investments by hyperscalers—Google, Meta, Microsoft, and Amazon—as of June 2024. It highlights instances where these companies are major capacity buyers, part owners, or sole owners of a cable and the year that that cable was or is expected to be Ready For Service. It does not include data on fibre pairs or leases of cable bandwidth that these companies may have acquired on other cables. (Data sources: Telegeography, Submarine Networks)



Source: Image by ASPI authors, using data from *TeleGeography*, *Submarine Networks*, and ASPI research.¹²

Power concentration in the AI ecosystem: Cloud market shares (Source: Procopio, 2024)



Big Tech pushing for escalation...(1)

The New York Times

'I Could Solve Most of Your Problems': Eric Schmidt's Pentagon Offensive

The former Google C.E.O. has reinvented himself as the prime liaison between Silicon Valley and the military-industrial complex.



Big Tech pushing for escalation...(2)

- ▶ **Schmidt et al. (2024), 'Defense Against the AI Dark Arts: Threat Assessment and Coalition Defense' (Hoover Institute policy-paper):**
- ▶ "There are the threats that could be posed by the **worst people and governments in the world** using the most advanced possible models...strategic surprise that might be developed by hostile states with models or developmental approaches **quite different from anything being developed by private companies in the free world...**
- ▶ **[AI] threat evaluation** requires a major effort that goes well beyond what governments are doing now...will require work with the most advanced models that we have made or that others could make...**governments now do not have the technical teams or the infrastructure to do this work...**"

Big Tech pushing for escalation...(3)

- ▶ "Frontier AI capabilities will become part of the defense industrial base of the free world, indispensable in evaluating dangers and developing countermeasures...governments will have to rely on the private sector to help build up the most advanced capabilities in the world, so that governments can then access, supplement, train, or fine-tune those capabilities to defend against dangers that may go beyond anything the companies conceive for their own private purposes..."

And to redefine the contours of the military-digital complex...(4)

- ▶ "...we must get started building the [base camp](#)...the next stage of relations between governments and industry at the AI frontier...If governments help sustain the companies essential to their defensive work, they may ask companies to accept certain obligations to protect the public interest..." (Schmidt et al., 2024)

And to redefine the contours of the military-digital complex...(5)

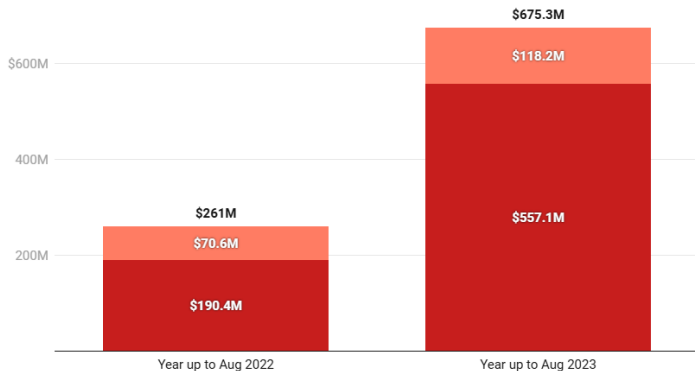
- ▶ The 'nuclear parallel':
- ▶ "...[like] [Eisenhower's Atoms for Peace initiative](#) original conception, when the United States (and the Soviet Union) offered peaceful uses of nuclear technology in exchange for countries agreed to forgo military uses...In one [AI-inspired reconception](#), leading AI-producing countries would share the benefits from safe AI in exchange of safeguards...the agreement might be enforced by export controls of key hardware or efforts to constrain cloud computing and reliance on insecure data centers" (Schmidt et al., 2024)

A strategy which seems to pay off...(1)

U.S. military AI spending nearly tripled from 2022 to 2023

Total dollars obligated from AI-related federal contracts, \$M

■ Department of Defense ■ Other agencies



A strategy which seems to pay off...(2)

- ▶ A selected set of Big Tech bosses (or affiliates) to play a key role in the incoming Trump administration:
- ▶ [Elon Musk \(X, Space-X, X-AI, Tesla\)](#) → key role in the new government, in charge of 'reforming' the Federal administration yet his role seems to go well beyond...
- ▶ [Marc Andreessen \(A16Z\)](#) → major Trump donor, exclaiming on X as election results start consolidating 'FUCK yes. The romance of production is back'...
- ▶ [Andrew Ferguson as the new head of the Federal Trade Commission](#) → rolling back Lina Khan's attempts to more strictly regulate Big Tech
- ▶ [Jacob Helberg as undersecretary of state for economic growth, energy and the environment](#) → China hawk and against Big Tech 'censorship' yet in no way against platforms monopolistic power

Challenges for the governance of AI

- ▶ The overall role of AI in the economy and society → who set the rules of the game? who drives the technological frontier?
- ▶ AI and the growing concentration of market power → consolidating incumbents' (i.e., Big Tech) position and stiffening hierarchies
- ▶ AI and the military-digital complex → technologies for war or for the common good?
- ▶ The 'elephant in the room' → urgent need to analyse, understand (and compare with the US one) the Chinese military-digital complex!