Il complesso militare-digitale

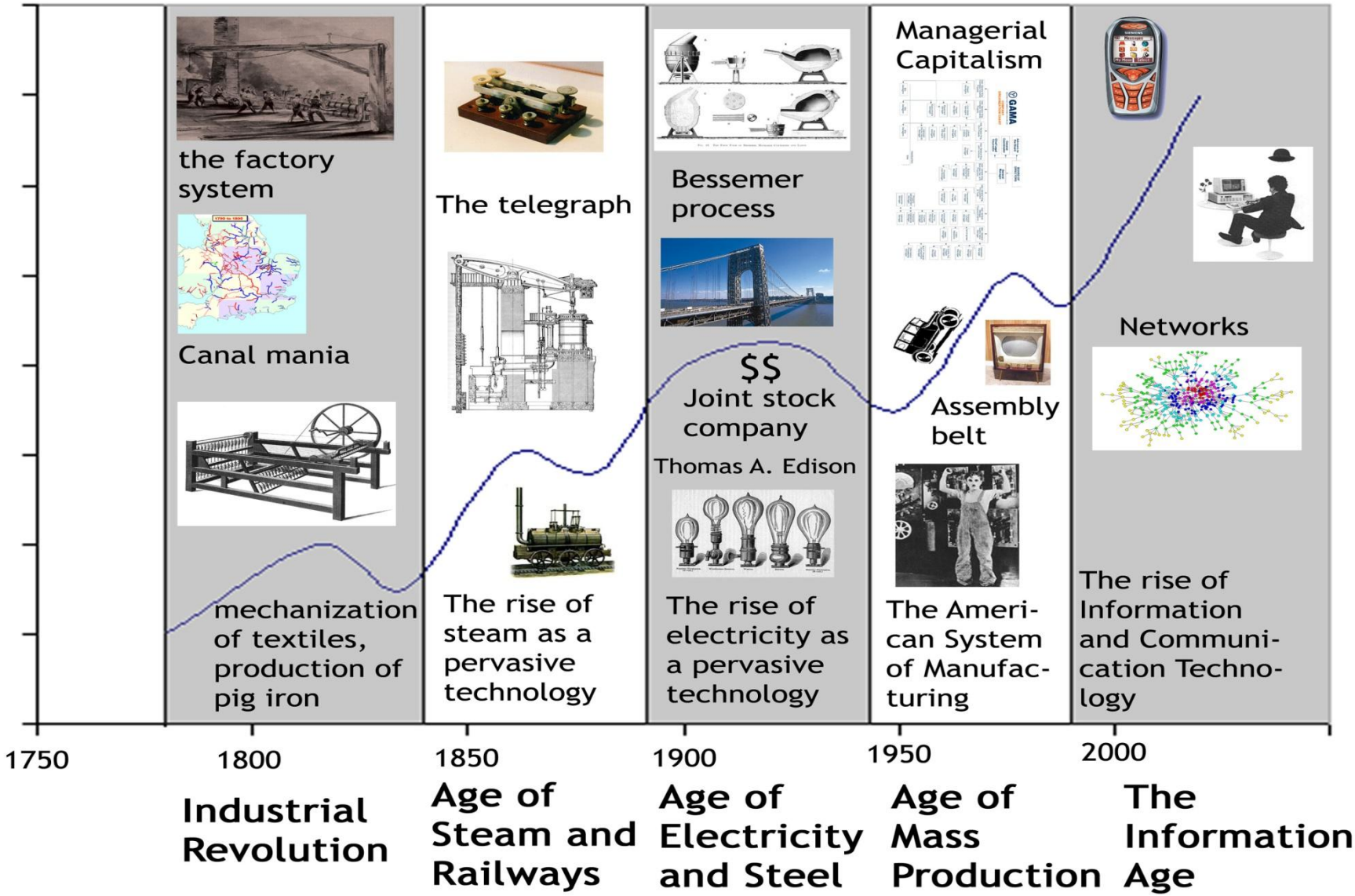
Mario Pianta
Scuola Normale Superiore

Sentieri di pace alla Sapienza, Fisica, Febbraio 2026

Technological paradigms

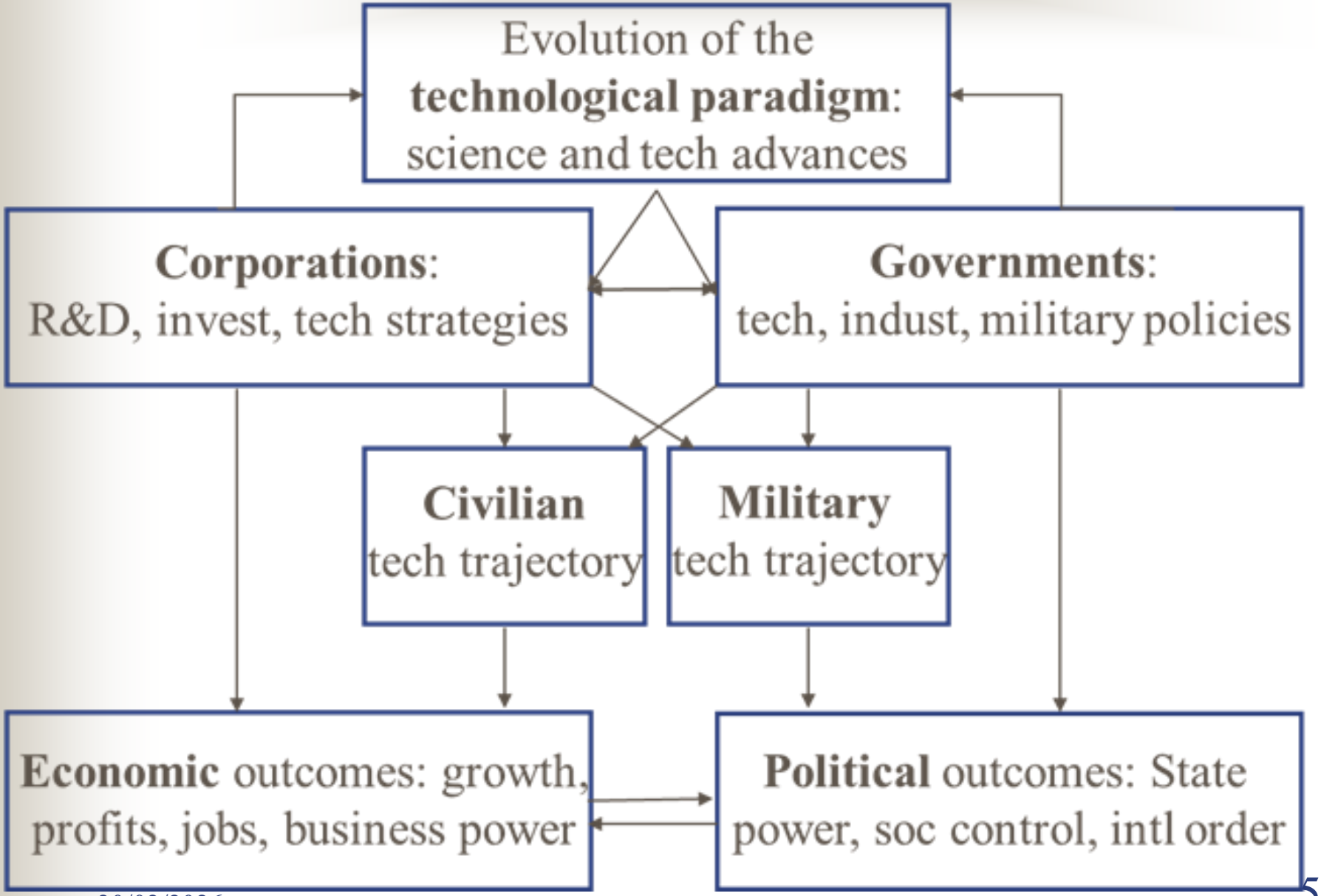
Freeman and Louca, As time goes by, 2001

- A **technological paradigm (Freeman, Perez)** is a set of technologies with pervasive applications and with rapidly decreasing costs.
- Importance of **matching** technological development and social-institutional context
- Strong **productivity** growth, new products, new markets, new managements models
- **Conflict** with previous tech paradigms, social arrangements, policies


the factory system
Canal mania
mechanization of textiles, production of pig iron
The telegraph
The rise of steam as a pervasive technology
Bessemer process
$$
Joint stock company
Thomas A. Edison
The rise of electricity as a pervasive technology
Managerial Capitalism
Assembly belt
The Ameri-can System of Manufac-turing
Networks
The rise of Information and Communi-cation Techno-logy
1750
1800
1850
1900
1950
2000
Industrial Revolution
Age of Steam and Railways
Age of Electricity and Steel
Age of Mass Production
The Information Age

Civilian vs military tech

- There is a contrast between civilian and military goals, diversity of technological trajectories. **Civilian** trajectories are market driven, constrained by the pressure for cost minimisation, wide applicability and mass consumption, and are shaped by competition among several oligopolistic players. **Military** trajectories are shaped by requirements of the military, command and control, maximum performance requirements, little attention to cost and frequent inefficiencies


Evolution of the
technological paradigm:
science and tech advances
Corporations:
R&D, invest, tech strategies
Governments:
tech, indust, military policies
Civilian
tech trajectory
Military
tech trajectory
Economic outcomes: growth,
profits, jobs, business power
Political outcomes: State
power, soc control, intl order

Impact and diversity of models

- Impact on countries' specialization
- Military vs civilian manufacturing:

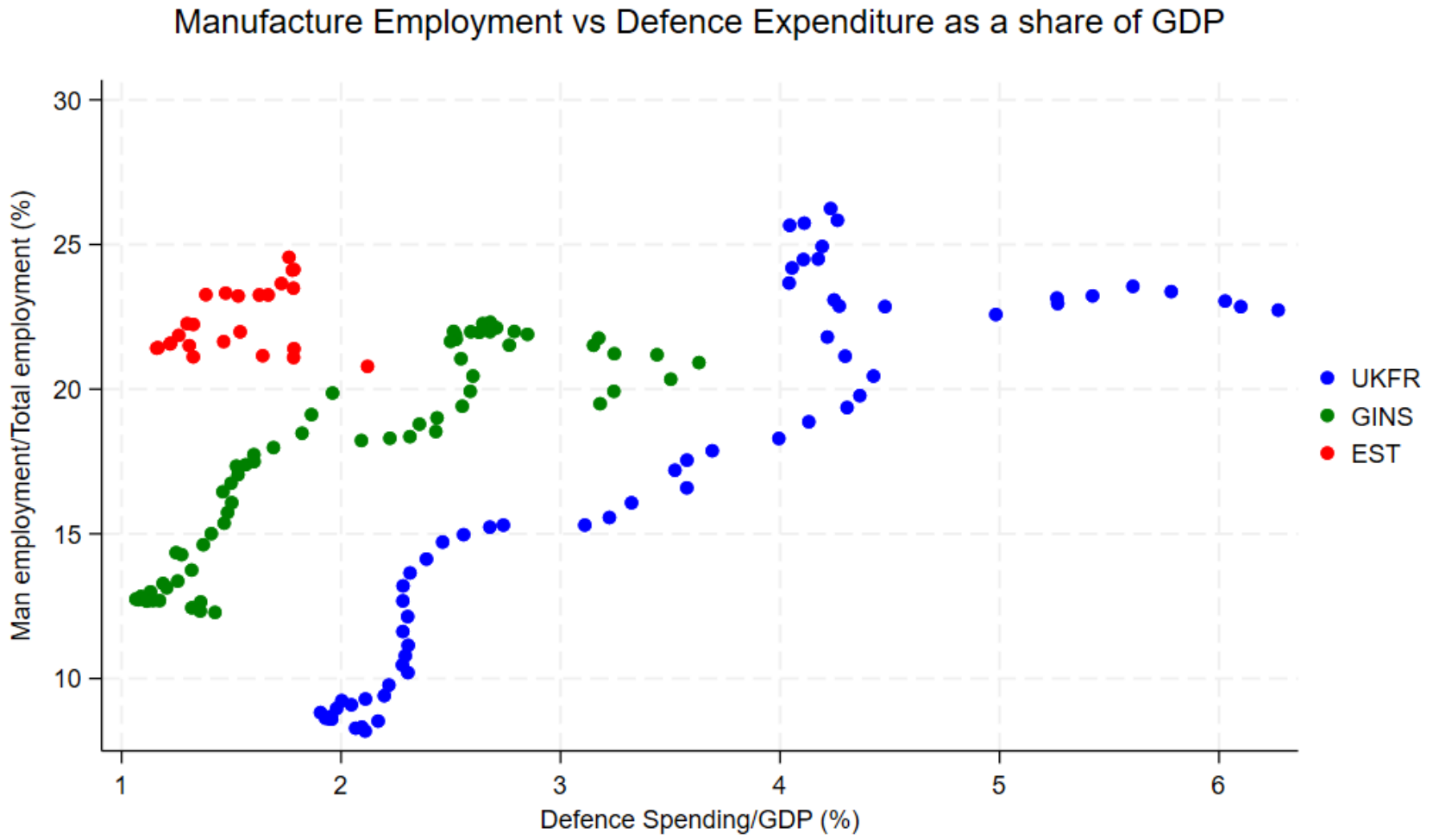
Decline of US, rise of Japan, EU, China

In EU: UK, France vs Germ, Ita, Spain

- Political and military power vs econ performance
- Governments' publ exp, industrial and technological policies are crucial

Different trajectories of deindustrialisation/mil exp

UK-Fr vs GINS vs East EU



Il cattivo esempio Usa

- Rosenberg: «major innovations were not achieved on projects supported by military R&D. Military R&D on possible alternative routes to miniaturization were largely spent 'betting on the wrong horses'"
- Nuclear energy, supersonic travel:"the indiscriminate pursuit of military spillovers turned out to be a recipe for commercial disaster when optimal design requirements of the military and civilian sectors were sharply divergent" *(ibid.:* 24).(Rosenberg, 1986)
- Nelson: "the military and space programmes surely do not provide us with a model for future policies in support of high technology industries"
- Mary Kaldor: The Baroque Arsenal

Le politiche Usa all'avvio del digitale

- The emergence of the new ICT paradigm was a key theme of contention between alternative technological strategies, with a dramatic divide between military and civilian directions.
- In the 1980s the US had major industrial policies for microelectronics, fifth-generation computers, telecommunications, a policy of strict controls over the transfer of military-relevant technologies to the Soviet Union, enforced by the CoCom (Pianta, 1988).
- In 1983 the US launched the largest research programme ever financed by a Western government – the Strategic Defence Initiative, 'Star Wars', $33 billion over the 1984-90 period
- Pressure on EU, Japan

La risposta europea degli anni ‘80

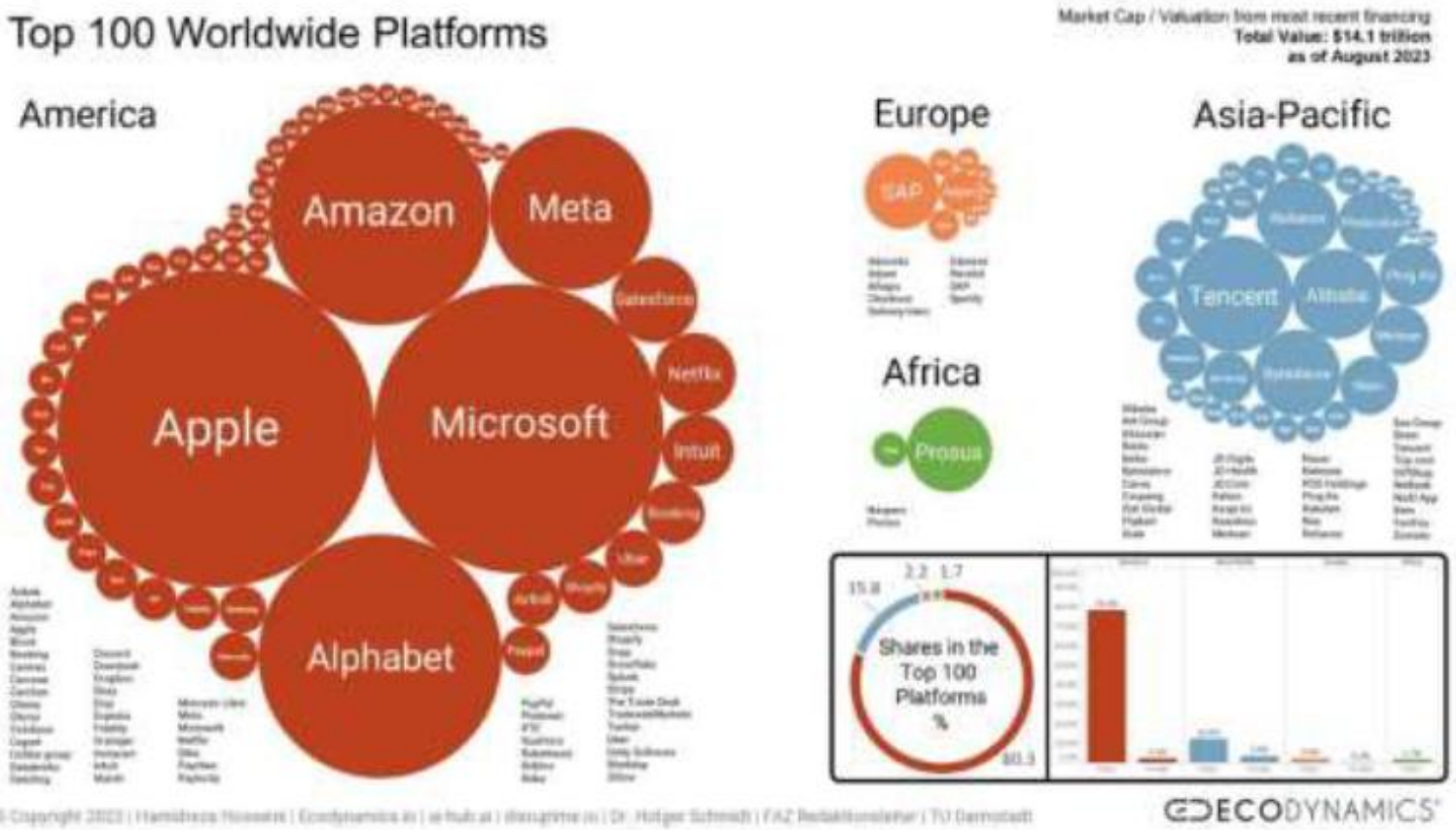
- In the 1980s, the policy responses from Europe and Japan emphasized civilian priorities.
- **European Community**: common research programmes mainly in civilian ICT areas: the 1987-91 'Framework Programme' of the European Commission, the Esprit programme in information technology and RACE in telecommunications. Another important French-initiated Europe-wide initiative, developed as a specific response to the US Strategic Defence initiative, was the Eureka programme, with a focus on ICT commercial technologies (Pianta 1988).
- **Japan**: Fifth-generation Computer Programme in ICTs, Frontier Research Programme and the Human frontiers science programme

The ICT technological paradigm: military vs civilian trajectories

- **Civilian dominance since the 1980s**:
- lower costs of chips, electronics, communication technologies, growing commercial markets, users
- decentralised computing model (personal computers, cell phones)
- Internet, data, networks, social media

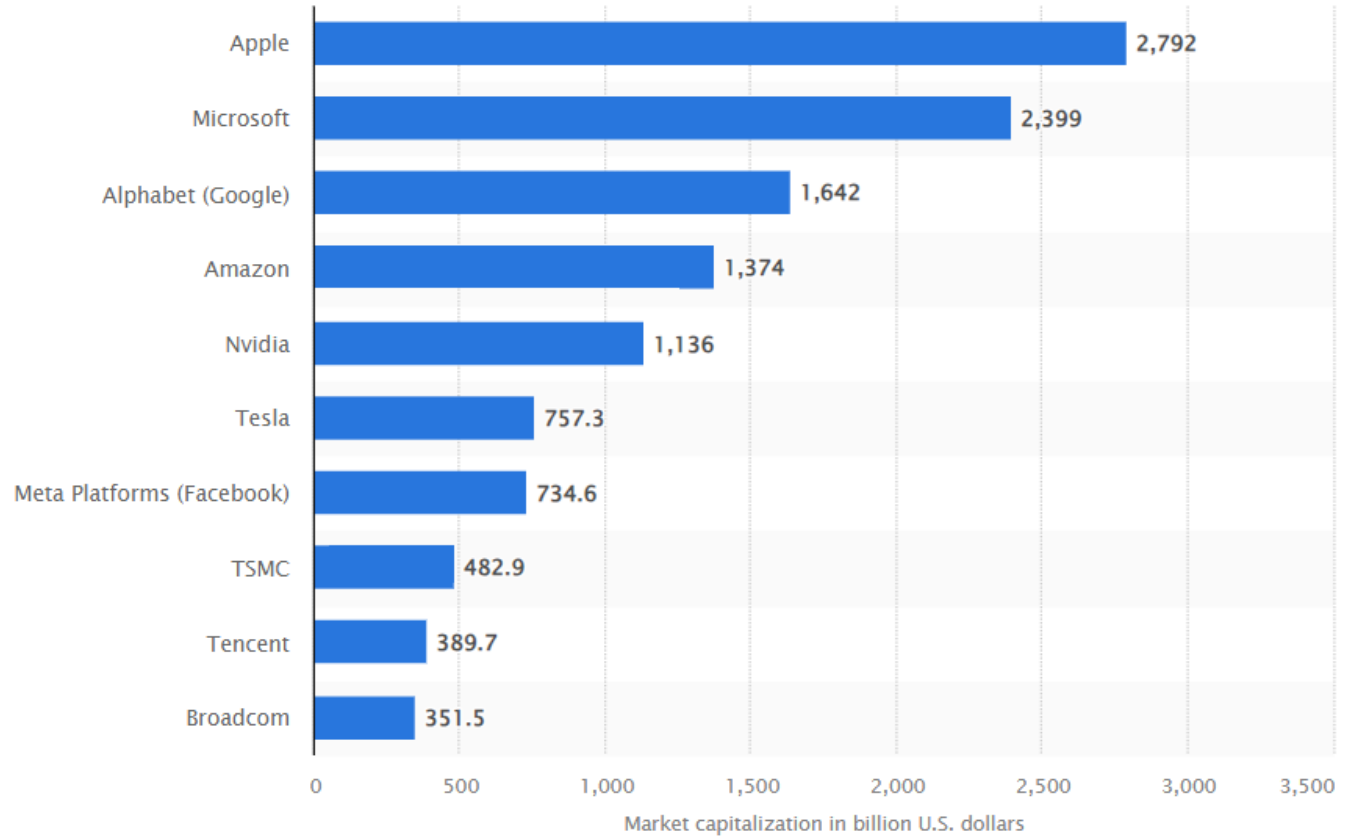
The rise of digital platforms

- The ICT paradigm leads to digitalisation and platform model: global networks, tailored services, commodification of personal data, 'surveillance capitalism' (Zuboff, 2019), large expansion of new civilian activities
- High financial dimension: market capitalization larger than the GDP of countries like Japan → (apparently) platforms do not need funds from military contract...is it true?
- Reshaping the operation of knowledge and innovation networks/ecosystems (e.g., Gawer and Cusumano, 2014; Jacobides et al., 2024)→strengthened rather than challenged by innovation-based competition (Kurz, 2023)
- Surveillance-based business model (Zuboff, 2019) challenging the very conceptualization of the firm (Pitelis, 2022, 2025)
- Exacerbating the process of labor fragmentation, increasing inequalities (Schor and Vallas, 2020)


Top 100 Worldwide Platforms
Market Cap / Valuation from most recent financing
Total Value: $14.1 trillion
as of August 2023
America
Amazon
Meta
Apple
Microsoft
Alphabet
Europe
SAP
Africa
Prosus
Asia-Pacific
Tencent
Alibaba
Shares in the Top 100 Platforms %
ECODYNAMICS

La capitalizzazione di Borsa

Nvidia ha una capitalizzazione di borsa pari al Pil della Germania; Apple, Amazon e Microsoft hanno valori superiori al Pil dell'Italia.



Le capacità del digitale diventano importanti per le strategie militari

Capabilities of surveillance, remote-control and autonomous systems, system integration, data managmt, targeting, logistics

Manipulation of information and social control

Power of Big Tech: monopolistic power of few large digital firms meets the logic of State power and military priorities

Iraq, Afghanistan, local wars, cyberwars, US-China rivalry, Israel's wars: 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

Why digital technologies are now 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 surveilance technologies
  - ✓ Pursuing and preventing cyberattacks

The rise of the military-digital complex

▶ After a phase of (apparent) detachment, military expenditure (and R&D) are again a key driver of profit accumulation

▶ Mutual dependency: the State cannot do without Big Tech (economic size and systemic nature, infrastructure, technologies, idiosyncratic capabilities) both in the civilian as well as in the military domain; Big Tech need the State to maintain their hold on markets, prevent hostile regulations, siphon out public resources

▶ A reshaping of the military-industrial complex (D. Eisenhower)? Tech transfer from the civilian to the military domain increasingly crucial, changing public procurement processes, pivotal role of Big Tech (together with a bunch of military-focused digital corporation, e.g. Palantir) in mobilising knowledge and innovation efforts

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...

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"

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

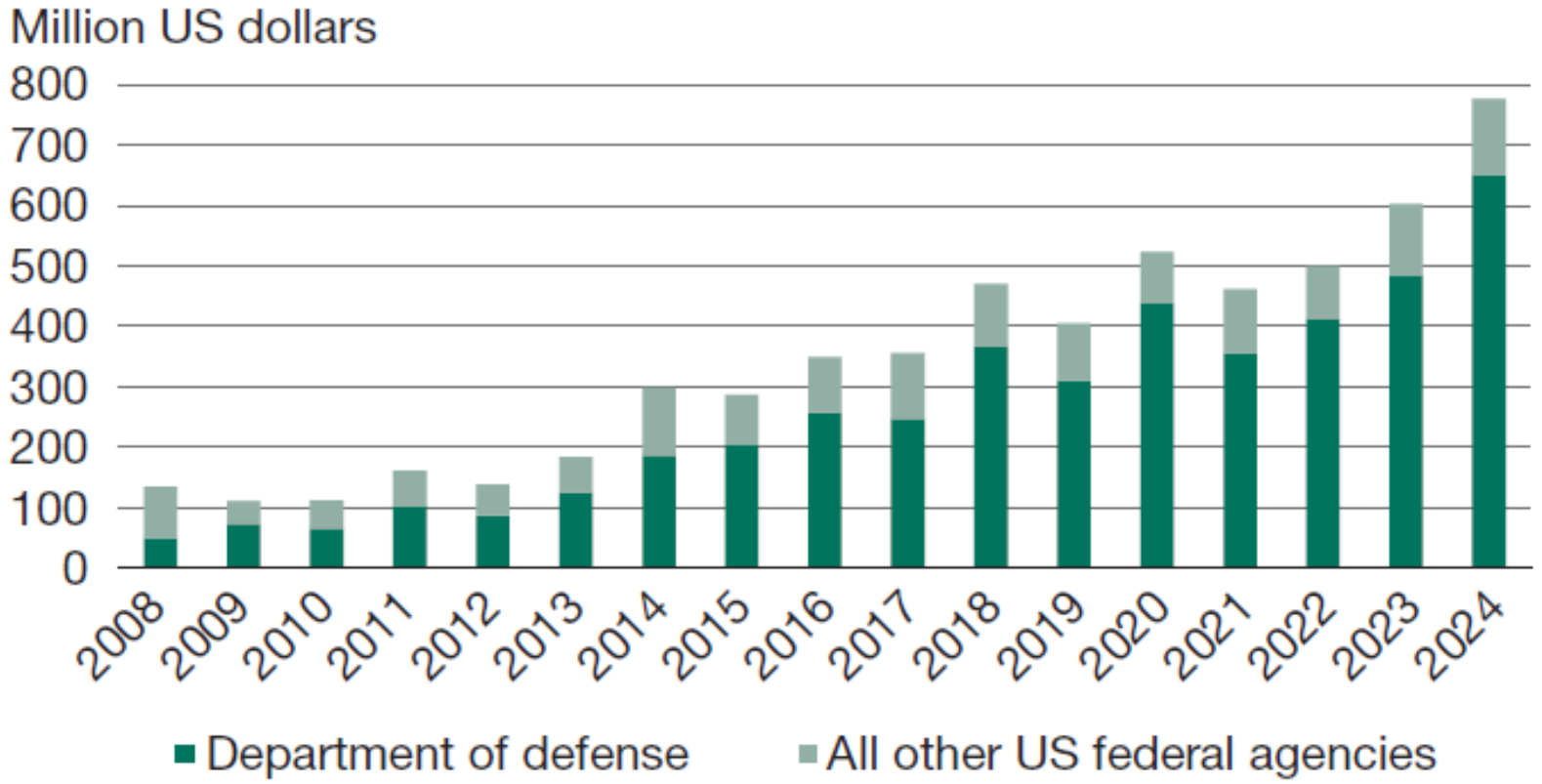


Table 1. Selection of multi-year military and security contracts signed by main US digital platforms.

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 US industrial and innovation policy

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-digital links

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

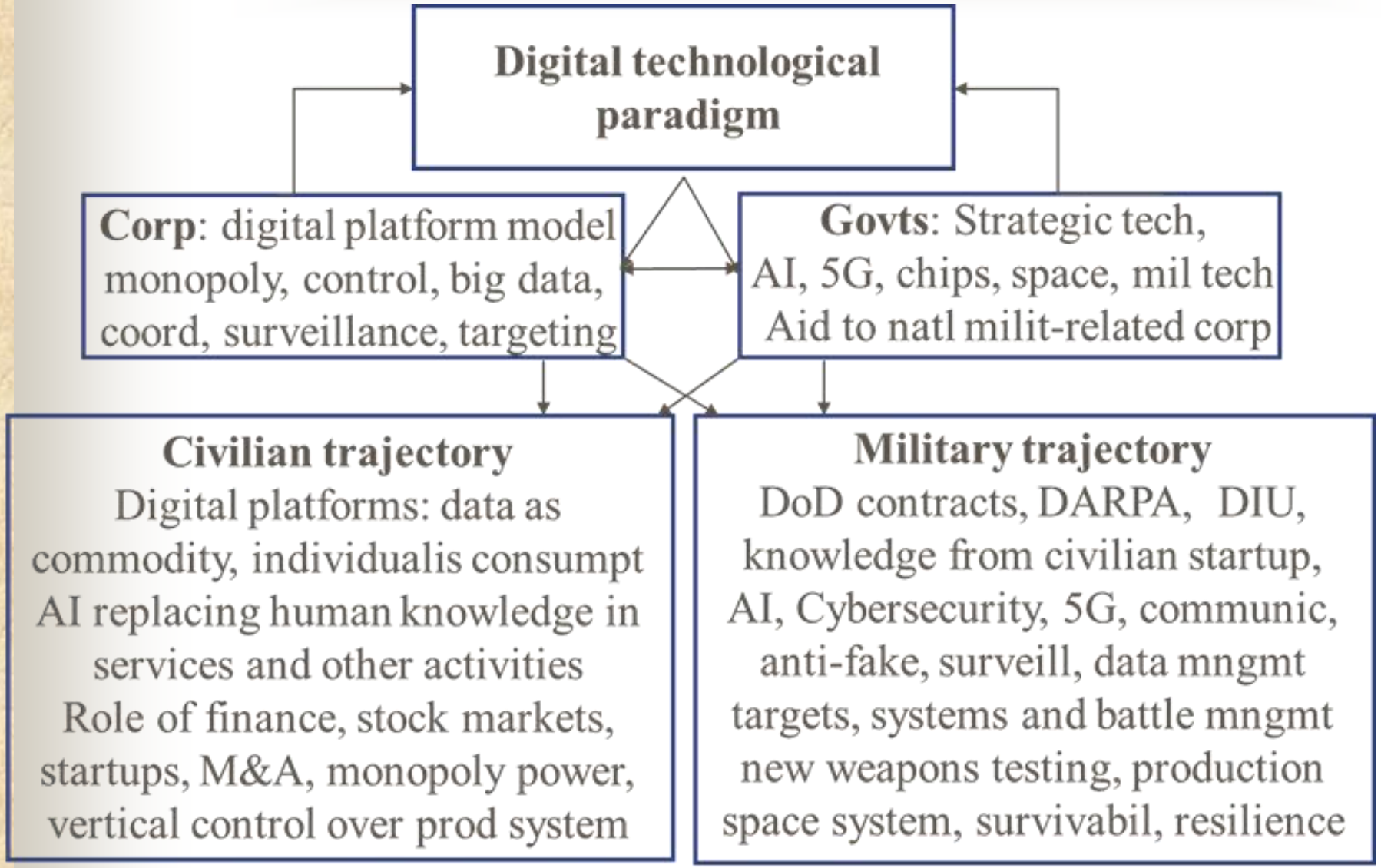
► Relevant cases, examples:

✓ 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


Digital technological paradigm
Corp: digital platform model monopoly, control, big data, coord, surveillance, targeting
Govts: Strategic tech, AI, 5G, chips, space, mil tech Aid to natl milit-related corp
Civilian trajectory
Digital platforms: data as commodity, individualis consumpt AI replacing human knowledge in services and other activities Role of finance, stock markets, startups, M&A, monopoly power, vertical control over prod system
Military trajectory
DoD contracts, DARPA, DIU, knowledge from civilian startup, AI, Cybersecurity, 5G, communic, anti-fake, surveill, data mngmt targets, systems and battle mngmt new weapons testing, production space system, survivabil, resilience

Eric Schmidt,former Google CEO

- “[AI] threat evaluation requires a major effort that goes well beyond what governments are doing now (…) 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 (...), the next stage of relations between governments and industry at the AI frontier” (Zelikow et al., 2024, Hoover Institution).

The danger of a militarized AI

Big Tech are 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

Conclusions

The military turn of Big Tech is problematic:

- Dangers for digital tech, econ, society
- Bigger dangers for AI
- Policy challenges, but who decides?

Parallel developments in China:

- Dangers of AI military rivalry

Need for action