

The military-digital complex: digital technologies and the new world (dis)order

Dario Guarascio¹

¹Sapienza University of Rome

2 October 2025

**War, peace and the world order
Scuola Normale Superiore, Florence**

Outline

Context

Digital technologies: civilian vs military trajectories

The political economy of the military-digital complex

The US case

A Chinese military-digital complex?

Discussion: clash between military-digital complexes, European weakness and the role of social conflicts

Context

- ▶ A new world (dis)order shaped by the conflict between two **military-digital complexes (the US vs China)**: *crisis* between Big Tech and the military apparatus
- ▶ Unprecedented **concentration of techno-economic power (Big Tech' size larger than economies as Germany or Japan)**, relentless fight to control markets, critical raw materials, infrastructures and (digital) technologies
- ▶ **Surveillance capitalism** (Zuboff, 2019) meets the 'digitalization of war'

The ICT technological paradigm: military vs civilian trajectories

- ▶ From 1960s, rise in information technology driven by **demand for military electronics** for aerospace and nuclear systems ('Sputnik shock' and Vietnam's war), ARPA, centralised model aiming at increasing command and control capabilities (e.g., IBM's mainframe), key role of military procurement and vertically integrated industry
- ▶ **1980s: lower costs of chips/electronics/communication technologies**, growing commercial markets, decentralised computing model (personal computers, dial-up technology and networks), from Arpanet to NSFNET
- ▶ **Star Wars** and concentration of US high-tech companies in military fields, powerful oligopolies, divergence between civilian and military trajectories → leadership of Japan (and then South Korea and China) in electronics, different industrial policy strategy (Japan and Europe focusing on civilian/commercial objectives, e.g., 'Frontier', 'Human Frontier Science' (Japan), 'Eureka' (Europe))

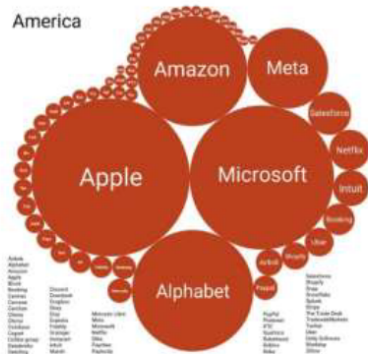
The rise of digital platforms

- ▶ **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)

Stylized facts: a polarized platform world

Top 100 Worldwide Platforms

America



Market Cap / Valuation from most recent financing
Total Value: \$14.1 trillion
as of August 2023

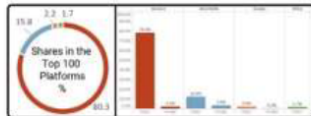
Europe



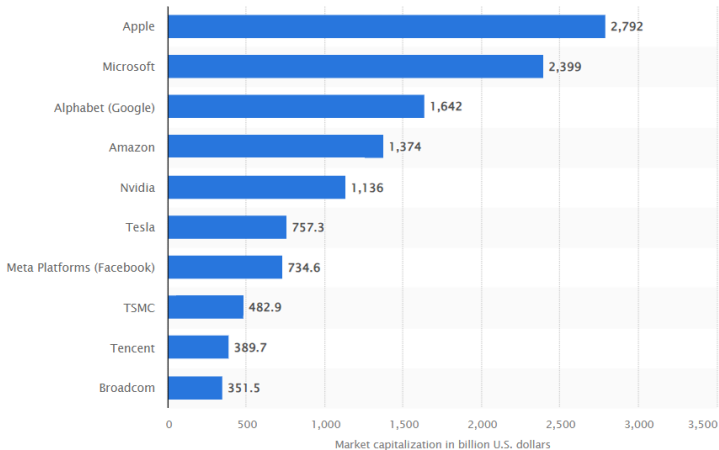
Africa



Asia-Pacific



Stylized facts: market capitalization (2023)



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)

Why digital technologies (particularly AI) are 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 political economy of the military-digital complex

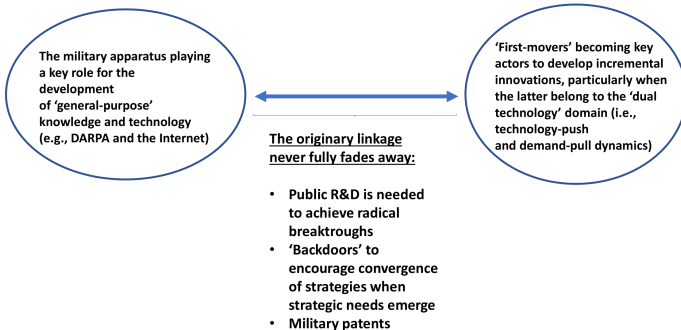
- ▶ After a phase of (apparent) detachment, **military expenditure (and R&D) are again a key driver of profit accumulation** (Imperialism and Monopoly Capital theories are back to the fore?)
- ▶ **Mutual dependency**: the State cannot do without Big Tech (economic size and systemic nature, infrastructure, 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

The US case (1)

- ★ The ‘originary linkage’ binding military apparatus and digital platforms:
- ▶ Big Tech owe their emergence to military projects (i.e., Arpanet) 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.

The US case (2)

The 'pendulum-like' relationship



The US case (3)

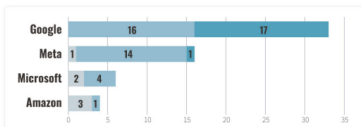
- ★ Knowledge, technology and critical infrastructures:
- ▶ Big Tech monopolize key assets (e.g., cloud, submarine cables), hold the majoritarian share of digital patents (Fanti et al., 2022) and are the loci where most of the formal and tacit knowledge is developed (Rikap et al., 2021)
- ▶ Military 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...

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)

 Major capacity buyer
  Part owner
  Sole owner



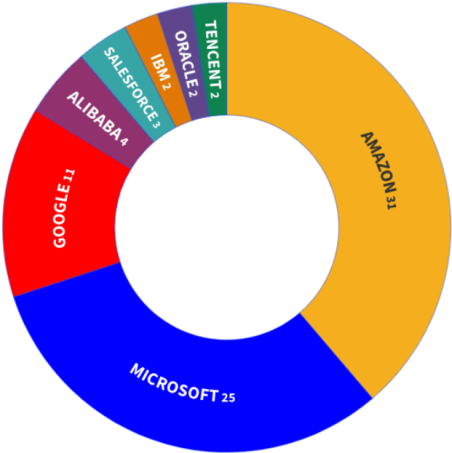
Acronyms

| | |
|---------------|---------------------------------|
| SJC | Southwest Asia-Japan Cable |
| AEC-1 | America Europe Connect |
| APG | Asia Pacific Gateway |
| NCP | New Cross Pacific Cable System |
| JGA-S | Japan-Guam-Australia South |
| PLCN | Pacific Light Cable Network |
| H/CC-2 | Hawkingsten/CelticConnect-2 |
| H/NSC | Hawkingsten/North Sea Connect |
| SJC2 | Southeast Asia-Japan Cable 2 |
| NPCI | North Pacific Connect Interlink |
| SPCI | South Pacific Connect Interlink |



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

Cloud market shares (Source: Procopio, 2024)



The US case (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)

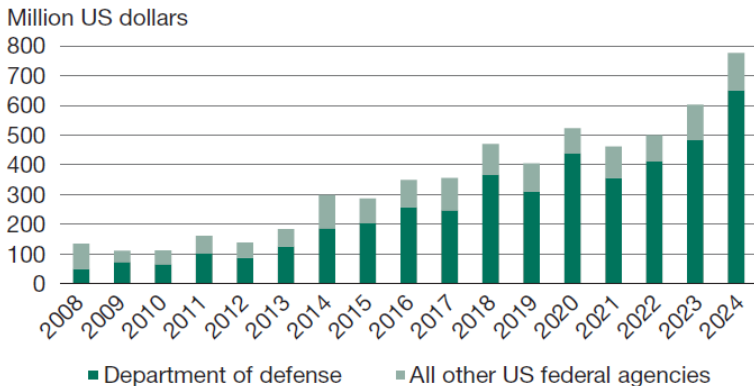
The US case (5)

★ 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"*

Big Tech's military procurement contracts

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



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

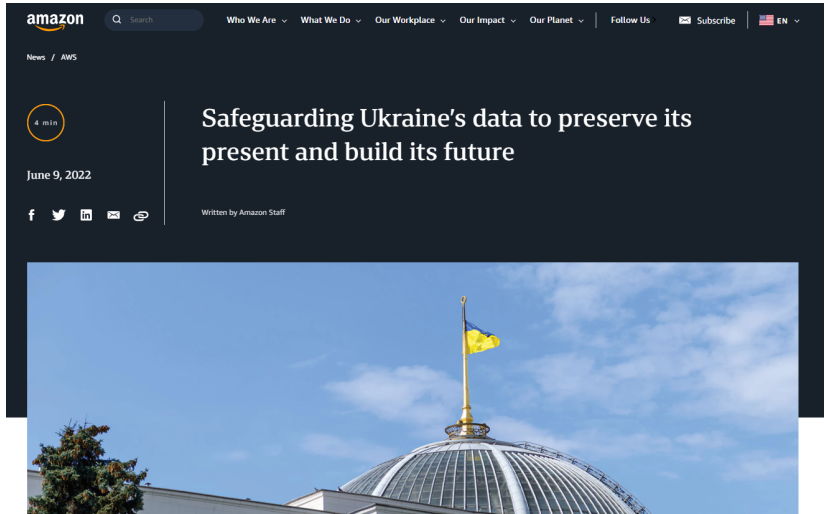
The military-Big Tech ‘revolving doors’

- ▶ **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: Ukraine

- ▶ **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: Ukraine




Big Tech go to war: Palestine

≡ **+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.

The Palantir's AI Platform for Defense

The screenshot displays the Palantir AIP (Artificial Intelligence Platform) interface, specifically the 'Battlefield Overview' view. The interface is divided into several sections:

- Left Sidebar:** Contains the Palantir logo, a link to 'Area of Interest /', and a section titled 'INTRODUCING AIP FOR DEFENSE'.
- Top Bar:** Features a green header with 'UNCLASSIFIED NOTIONAL DATA' and navigation tabs for 'AIP Terminal', 'Investigations', and 'Proposals'. It also includes a 'Share' button and a 'File Edit' menu.
- Main Content Area:**
 - Alerts:** A section titled 'Alert - Anomalous military activity detected' with a 'Show me more details' button. Below it, a 'Summary' box states: 'This satellite image was captured 8 minutes ago. An algorithm that detects military equipment found 5 pieces of equipment in the image.' A 'Details' box lists: 'Timestamp: 29 April 2023 14:39Z', 'Satellite: StarTech N-58200', 'Imagery Type: SAR', 'Image Quality: 1m', and 'Algorithm: Military Vehicle Detector V 25.3.0'.
 - SAR Imagery:** A satellite image showing a terrain with several orange markers indicating detected military equipment.
 - AI Assistant:** A section with a 'What military unit is in the region?' prompt and a 'Start typing something to explore with AIP...' input field.
- Right Panel:** A large map titled 'Battlefield Overview' showing a terrain with various military units and facilities marked. Key locations include 'Military Command', 'Camping Facility', 'Alert Region', '15th Artillery BN', 'Team Foxtrot', '72nd Airborne Brigade', 'Power Plant', and 'Team Omega'.

AI & the military-digital complex:

Where are we?

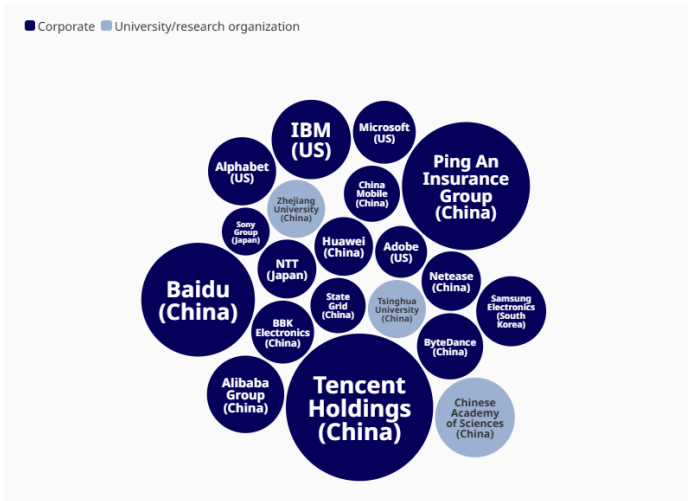
- ▶ AI technologies playing a pivotal role in contemporary warfare (e.g., autonomous weapons, drones, cyberattacks and surveillance) → increasing the [State-Big Tech mutual dependency](#) (see ‘Blurring boundaries’, Coveri, Cozza & Guarascio, 2024)
- ▶ As development (and management) of AI technologies 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 controls AI-related knowledge and technology?

Top patent owners (Source: WIPO)



A Chinese military-digital complex?

- ▶ **The only digital ecosystem comparable to the US one** → key role of PCC planning - industrial and technology policy - and selective openness
- ▶ **Chinese Big Tech** - Alibaba, Baidu, Huawei, Tencent - holding huge techno-economic power, mirroring their US counterparts
- ▶ **Big Tech-PCC:** mutual dependency (systemic nature of Big Tech and Chinese peculiarities, key role in driving China's economic and technological growth, regulation being crucial to support national platforms), unstable relationships (e.g., the Jack Ma's case...) and growing importance of military technologies (and related public expenditure)

The digitalisation of war and the PCC-Big Tech mutual dependency

Asia Pacific

Alibaba Joins China Arms Maker To Offer Location Services

By Agence France-Presse

Aug 20, 2015



The digitalisation of war and the PCC-Big Tech mutual dependency

- ▶ Big Tech controlling key dual infrastructure and technologies (pivotal to develop state-of-the-art semiconductors and AI), **supporting the PCC in expanding its sphere of influence** by strengthening dependency relationships (e.g., the digital Belt and Road initiative)
- ▶ Growing number of **Big Tech-military joint ventures**: Alibaba-NORINCO, Baidu-CETC, pioneering social control/surveillance systems (e.g., Alibaba sesame), active role in pursuing digital surveillance (e.g., Huawei in the Xinjiang province)
- ▶ **Institutionalisation of the military-digital complex and revolving doors**: the PCC's civil-military fusion (2015), China's defence in the new era (emphasis on AI, satellites and autonomous weapons), Big Tech CEOs included in top-level PCC committees

Discussion

- ▶ **Clash between military-digital complexes** (e.g., sanctions, export bans on critical technologies and Chinese retaliation on rare earths and dual magnets), growing risks of escalation (e.g., AI increasing escalation risks also in the nuclear domain)
- ▶ **Europe's weakness:** digital backwardness and technological/infrastructural dependency, wrong policy strategies (e.g., Readiness EU) and the illusion to challenge Big Tech's relying on regulation
- ▶ **Social conflict targeting Big Tech and its linkages with the military apparatus:** i) Alphabet' engineers blocking Project Maven (2016) ii) Alphabet, Amazon, and Microsoft employees against Big Tech-IDF cooperation iii) Chris Smalls (Amazon Union) joining the Freedom Flottilla iv) Waymo (Alphabet) robo-taxis set on fire during recent riots in Los Angeles

