The Military-Digital Complex: Digital Technologies and The New World (Dis)order

Dario Guarascio[1]

[1]Sapienza University of Rome

3 February 2026

Technische Universität Wien

DIGHUM Lecture series

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

- From 'endless globalisation' to a new world (dis)order shaped by the conflict between two military-digital complexes (the US vs China): *crasis* between Big Tech and the military apparatus fighting to control markets, technologies and critical raw materials

- Surveillance capitalism (Zuboff, 2019) meets the 'digitalization of war'...Hobson, Hilferding and Lenin's (digitised) Imperialism back to the fore?

- The military-digital complex fuels (and gains from) conflicts, contributes to the militarisation of the ICT technological trajectory as well as public discourse and industrial/innovation policies...

Stylized facts: De-globalization, slow-balization, regional fragmentation or what?

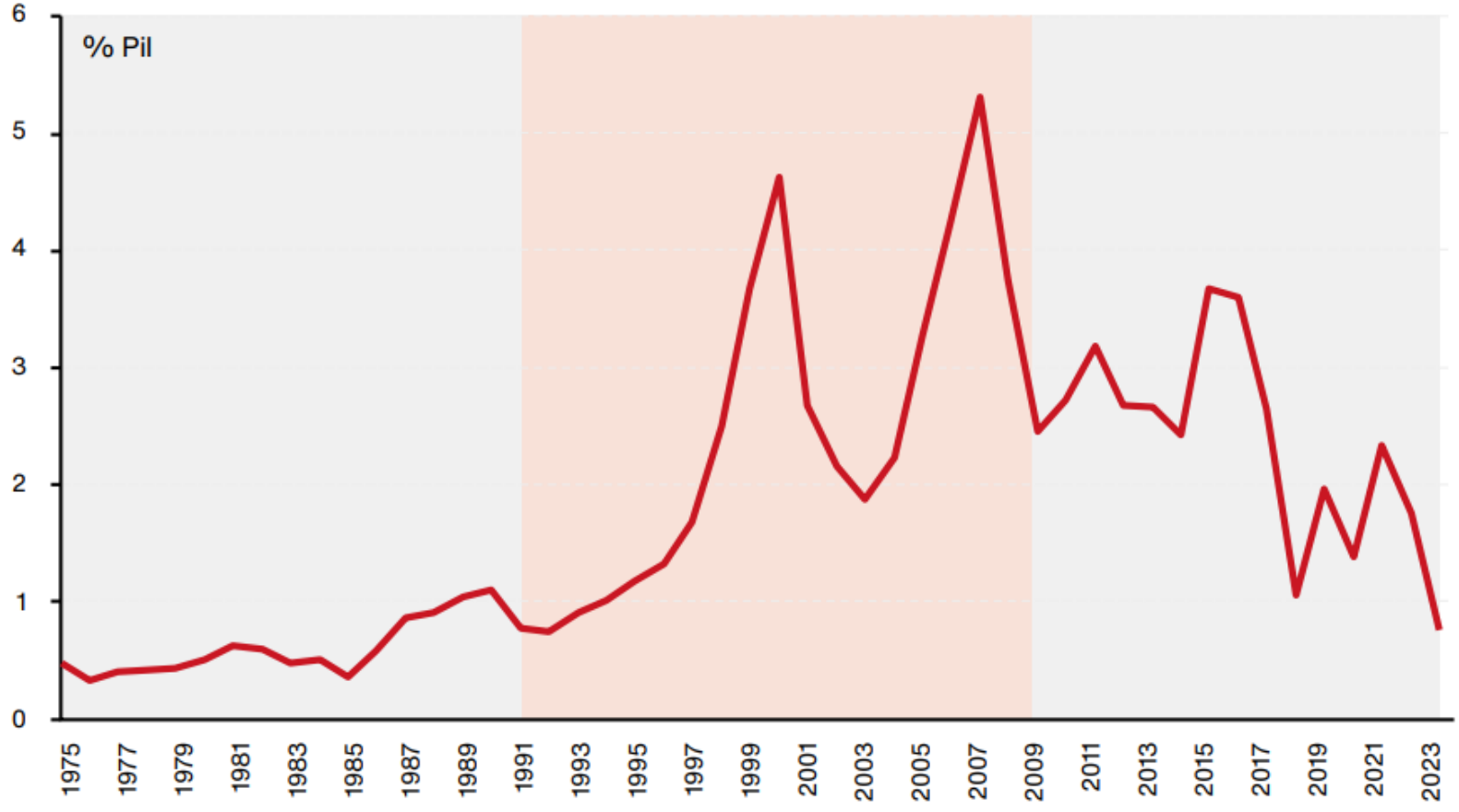
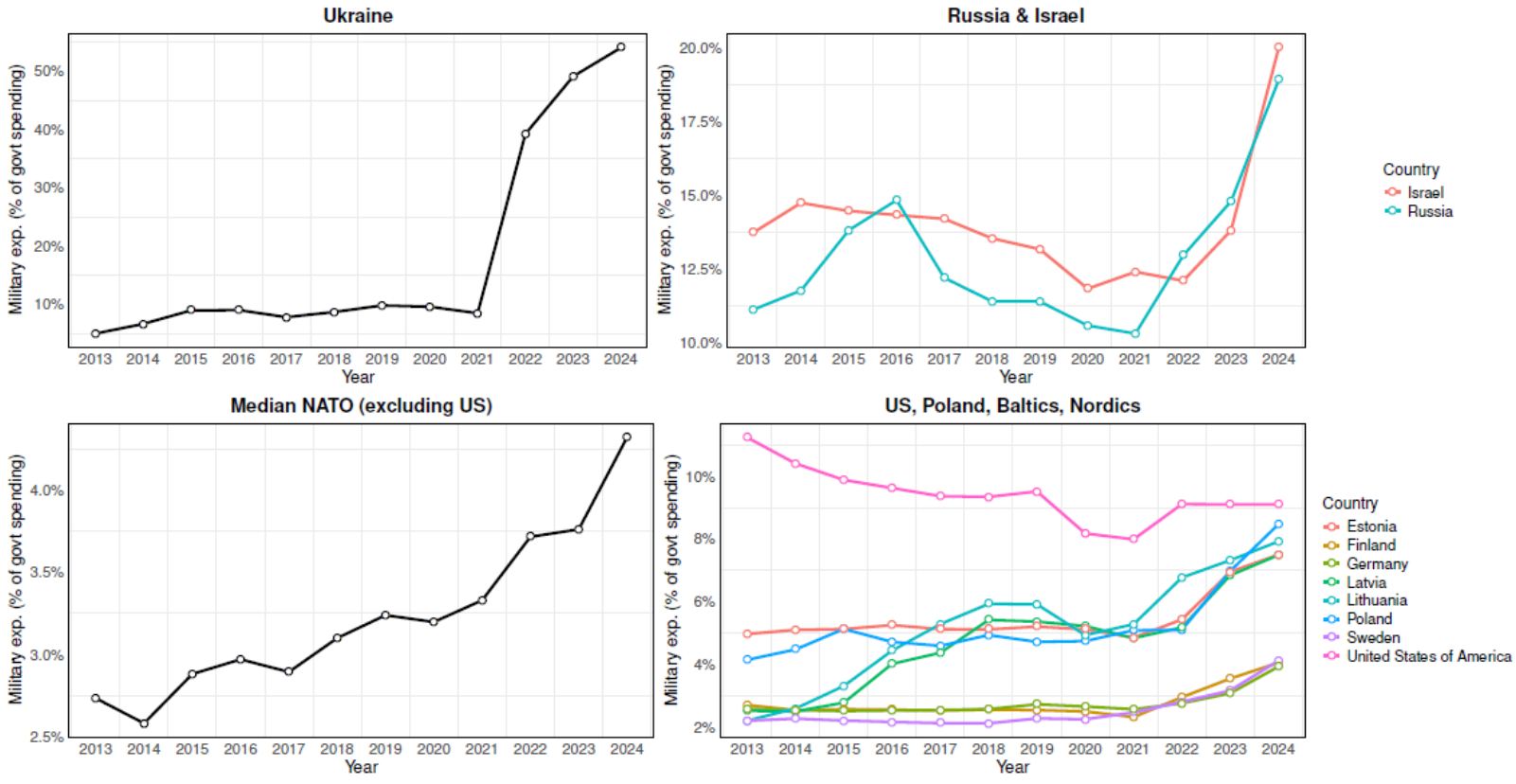
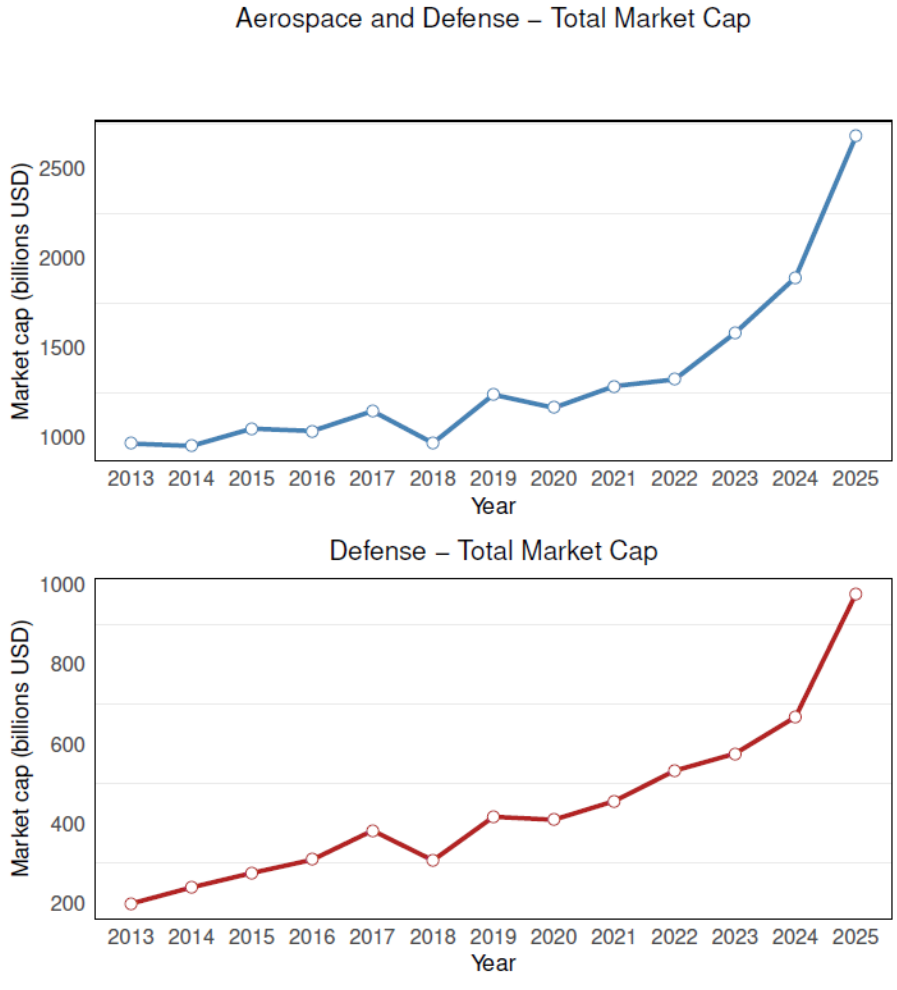


Figure: FDI flows as a share of global GDP (Source: World Bank)

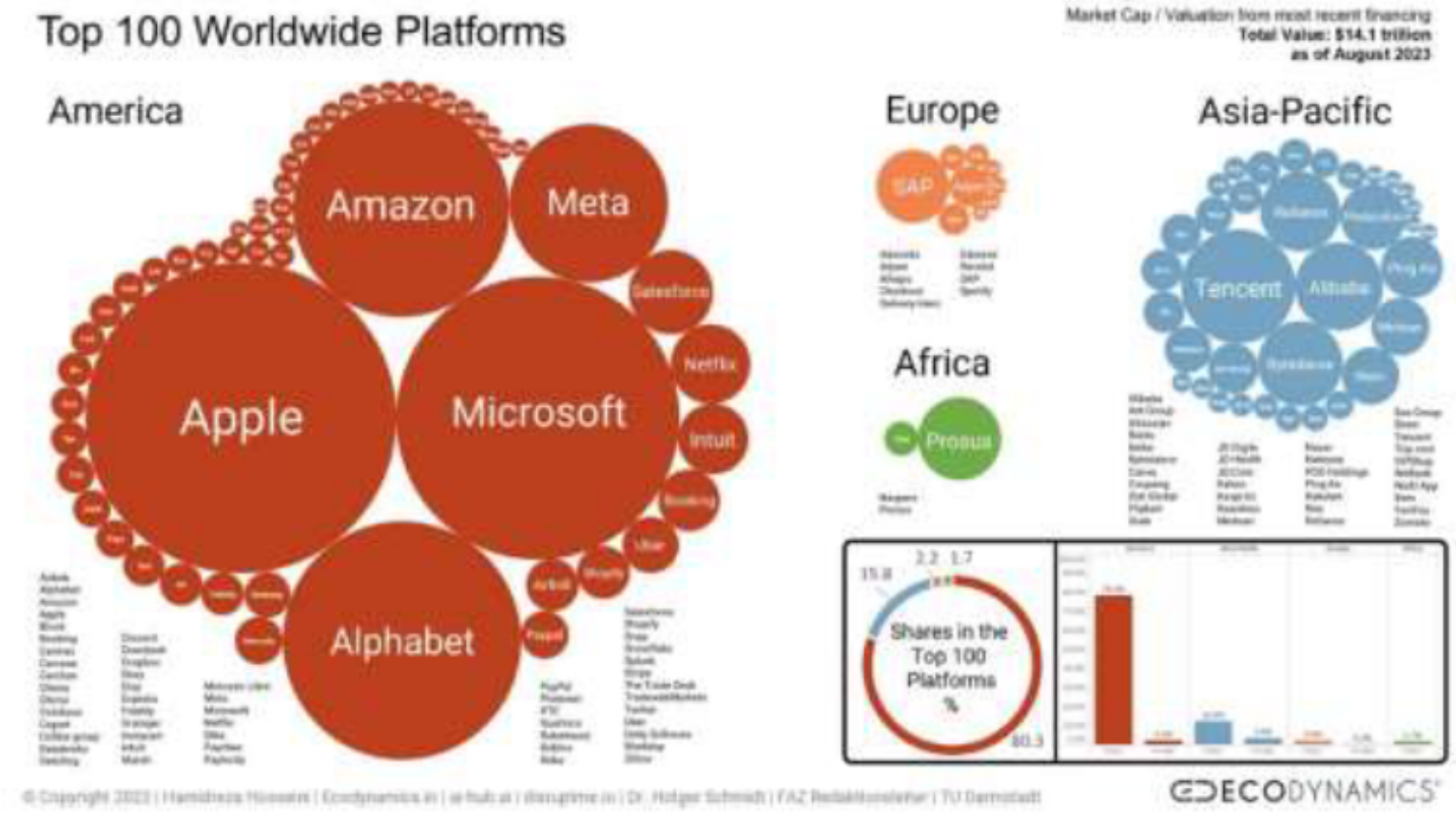
Stylized facts: A new warfare regime? (Bua, Dosi & Virgillito, 2025)



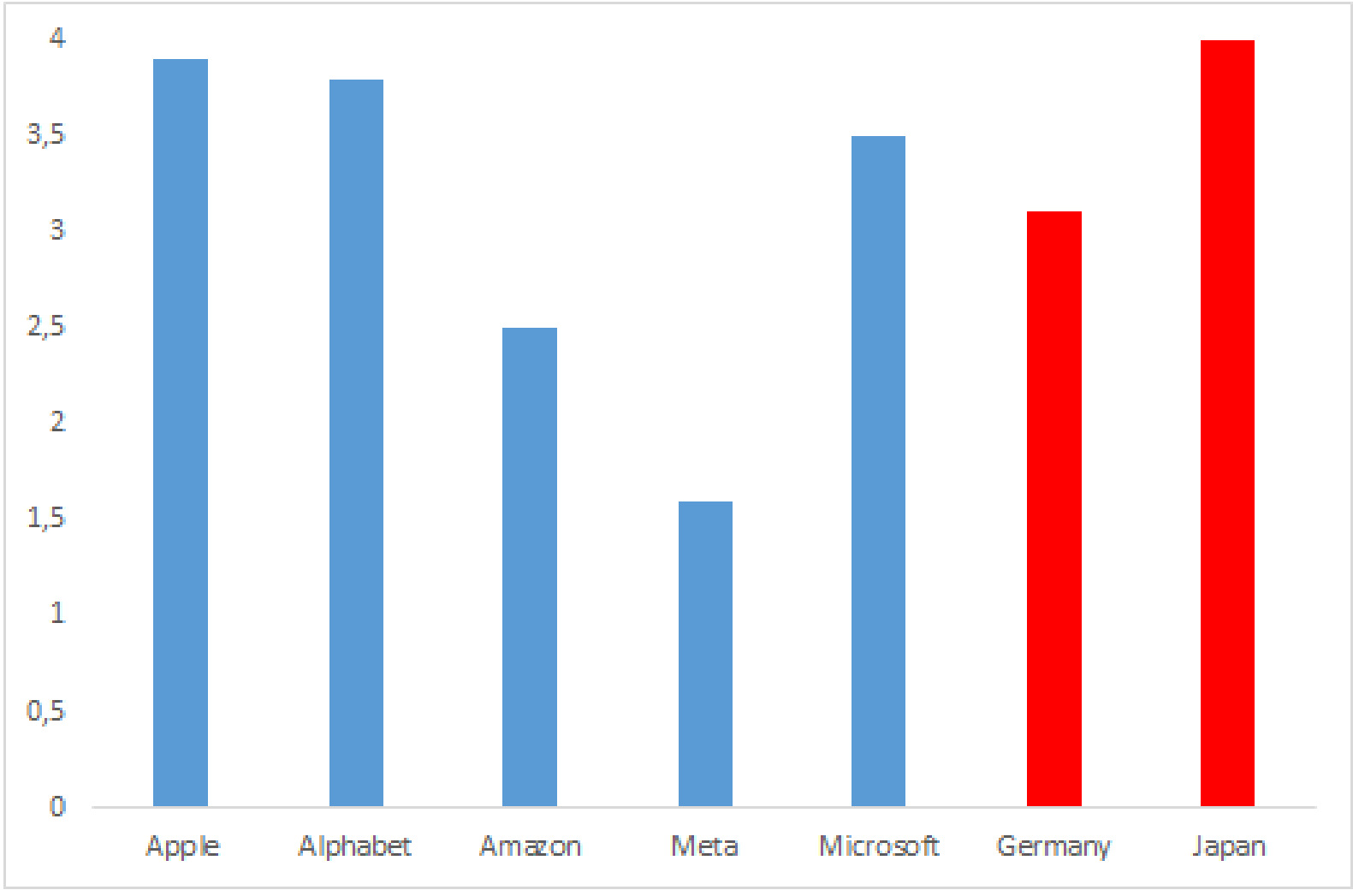
Stylized facts: A new warfare regime? (Bua, Dosi & Virgillito, 2025)



Stylized facts: A polarized platform world



Stylized facts: Big tech's market capitalization vs Germany and Japan's real GDP (2025)



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 $\rightarrow$ 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', large expansion of new civilian activities, network effects and winner-take-all mechanisms (Kenney et al., 2023)
- High financial dimension: market capitalization larger than the GDP of countries like Japan $\rightarrow$ (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) $\rightarrow$ 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)

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 $\rightarrow$ 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 surveilance technologies
  - ✓ Pursuing and preventing cyberattacks

The political economy of the military-digital complex (1)

- After a phase of (apparent) detachment, military expenditure (and R&D) are again a key driver of profit accumulation...Imperialism and Monopoly Capital (Baran & Sweezy, 1966) are back?

- Digitalisation *cum* platform-model: fueling inequalities, unprecedented concentration of techno-economic power, geographical polarisation, digital goods characterised by poor multiplier effects, lower capital- and FDI-intensity as compared to the 'Fordist era' (Ietto-Gillies, 2026)...military procurement as a way out of stagnation tendencies?

The political economy of the military-digital complex (2)

- 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

- Joining battlefields (e.g., Ukraine, Gaza) gives Big Tech unique opportunities to develop/refine new technologies, strengthen their bargaining power within the mil-dig complex, exploit their counterparts' technological dependency by providing 'infrastructures-as-a-service'

- A reshaping of the old 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 (3)

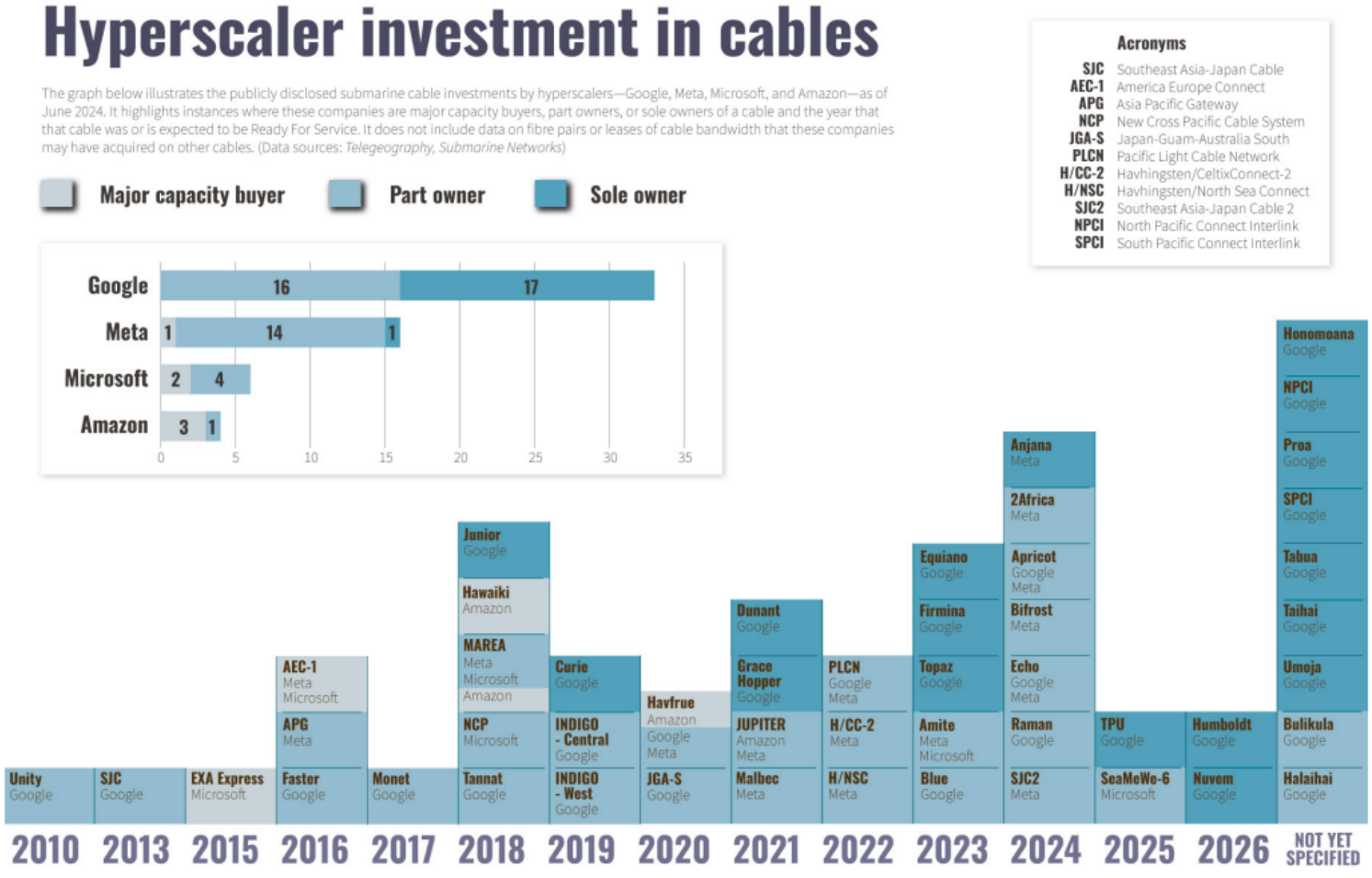
★ Knowledge, technology and critical infrastructures:

- 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

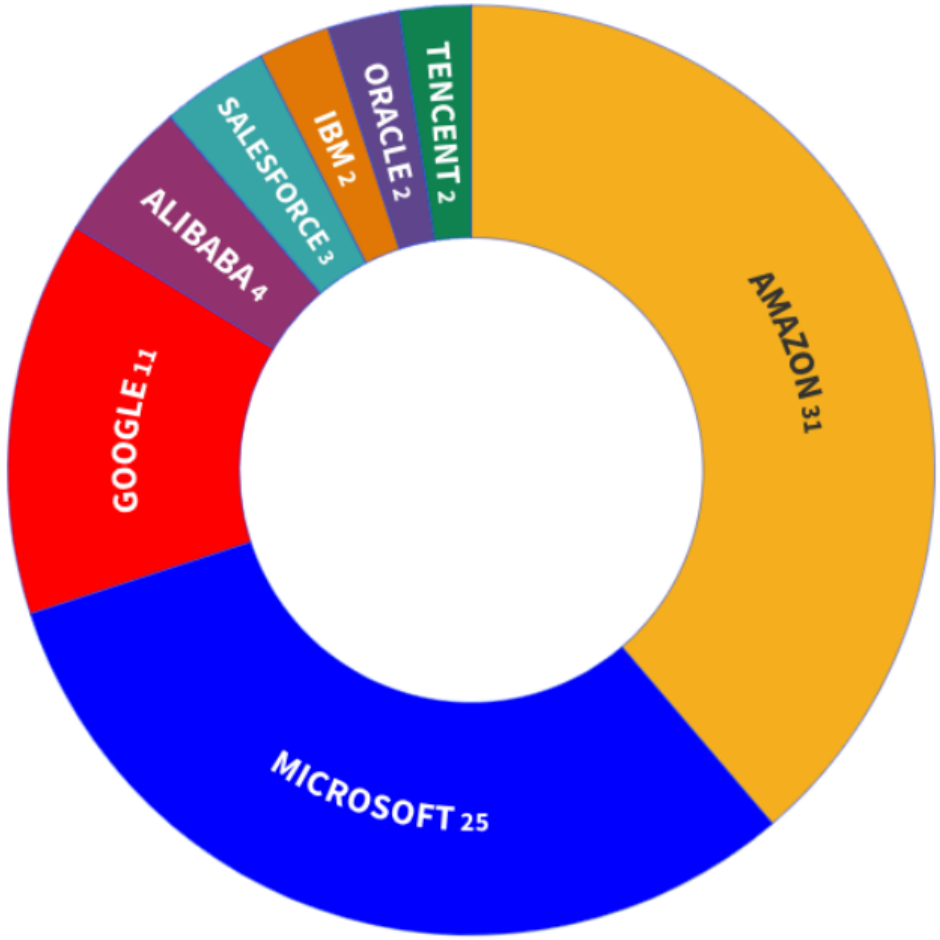
- Big Tech idiosyncratic competencies are key given their tacit and cumulative nature $\rightarrow$ as digital infrastructures grow in terms of size and relevance (e.g., increasing the mass of information stored and processed), the efficiency of embedded technologies (e.g., machine learning (ML) algorithms) and the uniqueness ('black-boxishness') of corporation-specific competencies increase too...

Submarine cables (Source: Telegeography)



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) $\rightarrow$ 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 $\rightarrow$ career prospects and incomparable economic levers (e.g., stellar salaries and stock options)

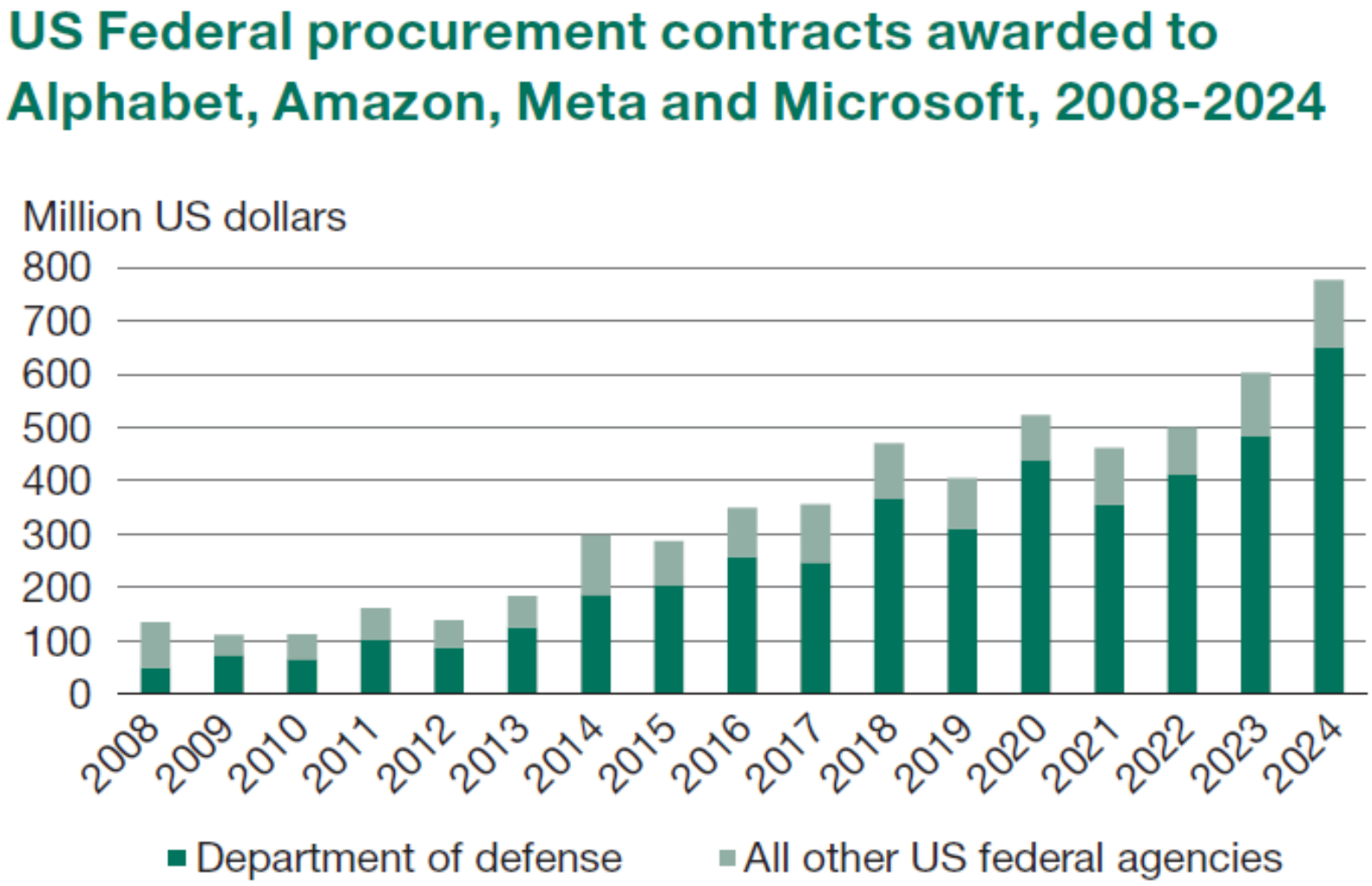
The US case (5)

★ 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



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:

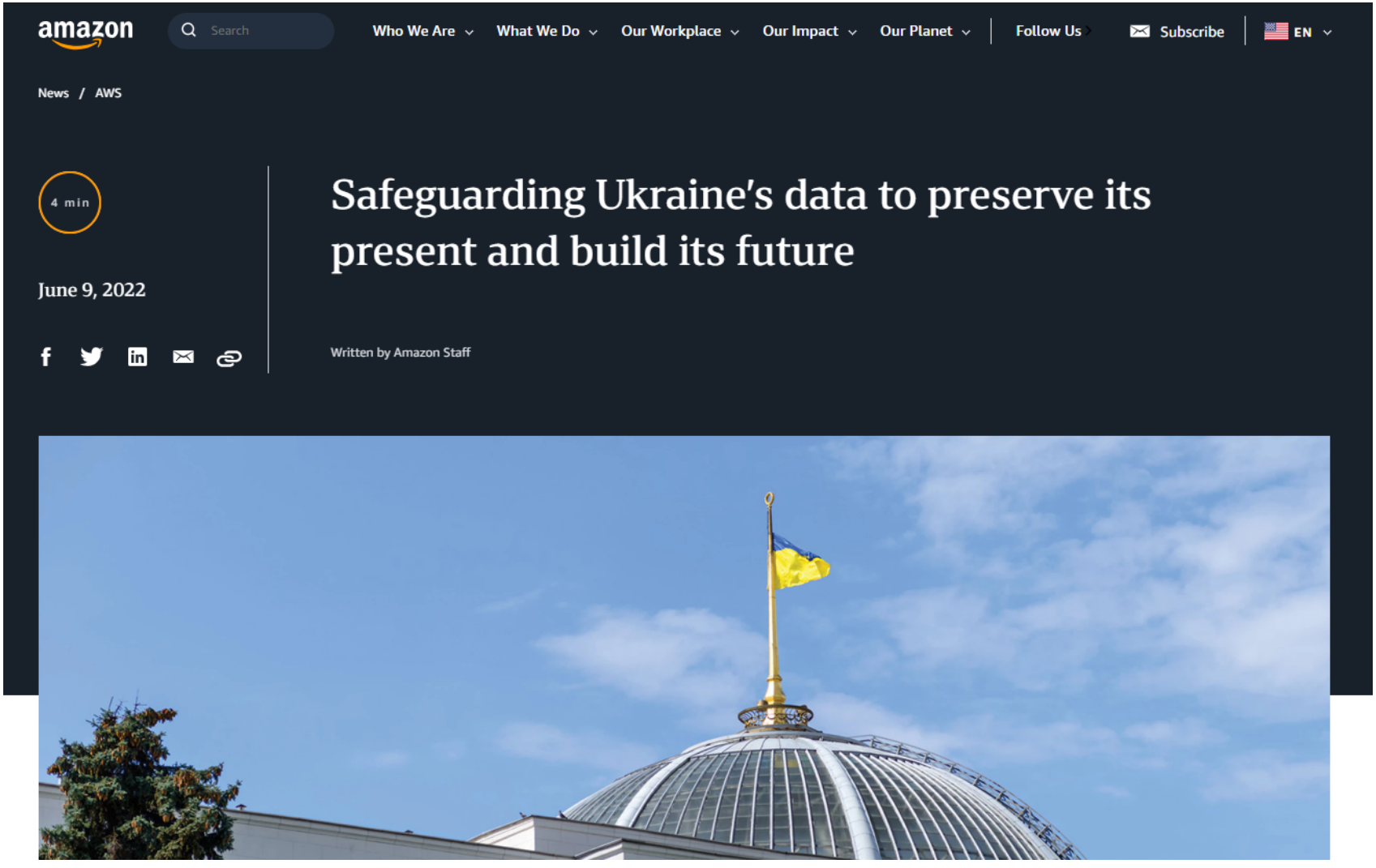
✓ Former Apple vice-president (Doug Beck) appointed as the new director of the Defence Innovation Unit (DIU)

✓ 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



Big Tech go to war: Ukraine

- Big Tech playing a key role on the (digital) battlefield: a large-scale destructive cyberattack has not materialized as US platforms provided crucial support to the Ukrainian military since the beginning of the war (Jacobsen & Liebetrau, 2025)

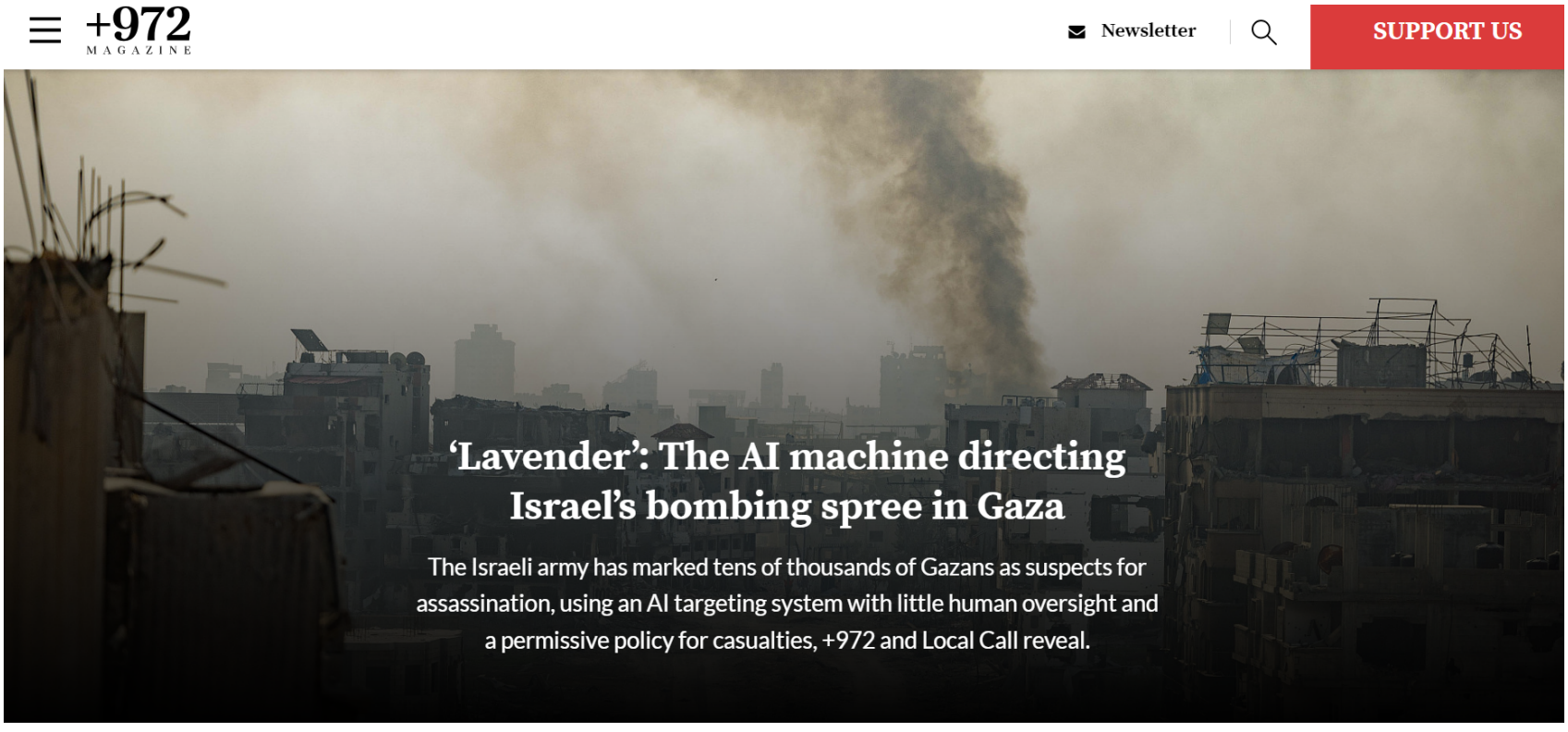
- Microsoft: designated teams to deliver end-point protection to Ukraine and shared its extensive knowledge on cyber threats with the Ukrainian military apparatus

- Amazon: moved Ukraine's IT infrastructure to their cloud storage facilities around Europe (Mitchell, 2022)

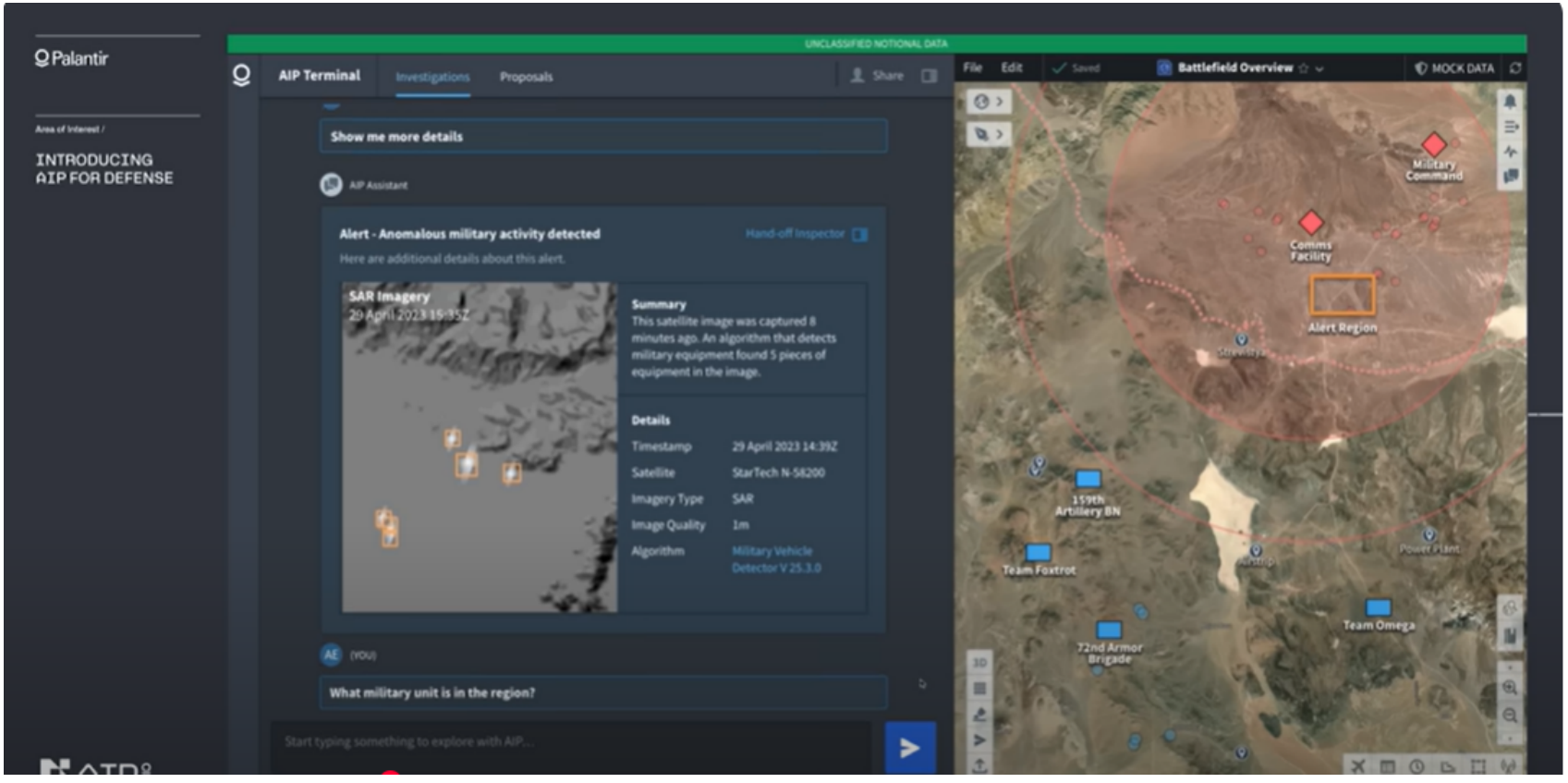
- SpaceX: starlink satellites enabled Ukraine to keep its critical communication running

- Apple block Apple Pay electronic payments and stop selling its products in Russia; while Facebook and Youtube halt Russian contents and state media channels such as RT and Sputnik from their platforms

Big Tech go to war: Palestine



The Palantir's AI Platform or Defense



Why does Big Tech's direct involvement in warfare activities matter?

- (Dual) infrastructure-as-a-service: highlighting the entanglement between physical/territorial and immaterial components of key infrastructures/technologies (cloud and data centers) and how this shapes State-Big Tech interactions within the military-digital complex (Jacobsen & Liebetrau, 2025)
- Blurring boundaries: Big Tech playing a crucial role (earning substantial profits, accessing data, developing military-specific services and gaining in terms of political leverage) well beyond traditional public-private distinctions due to their unique knowledge/capabilities (De Nardis, 2014); but States are just as important as data centers fall into their jurisdictions (Pedersen & Jacobsen, 2024)
- Learning and incremental innovations: joining the battlefield allows Big Tech to test new applications under extreme conditions (and without regulatory and safety constraints) accumulating valuable knowledge that can be eventually transferred to the civilian domain (De Petra, 2025)

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 (Jia & Kenney, 2022)
- 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 digitalisaton 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 digitalisaton 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 Xinjang province)

- Institutionalisation of the military-digital complex and revolving doors: the PCC's civil-military fusion (2015), China' 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


DARIO
GUARASCIO
Le Big Tech supportano strategie belliciste e partecipano direttamente alle attività militari e di intelligence. Lo Stato non può fare a meno delle loro capacità finanziarie, infrastrutturali e tecnologiche.
Imperialismo digitale
ECONOMIA E GUERRA AI TEMPI DELLE PIATTAFORME E DELL'IA
90 anticorpi Laterza
GUARASCIO Imperialismo digitale
Editori Laterza