AI, Trade, and Supply Chains

Opportunity, Risk and Judgement

Devon Whittle

DFAT, Trade Law and Economic Security Division planning day
20 October 2026



Introduction



GSi
GLOBAL SHIELD INSTITUTE

Part I

Opportunities

The AI supply chain and Australia’s position

Part II

Risks

Vulnerabilities and chokepoints

The National AI Plan

Three pillars:

1

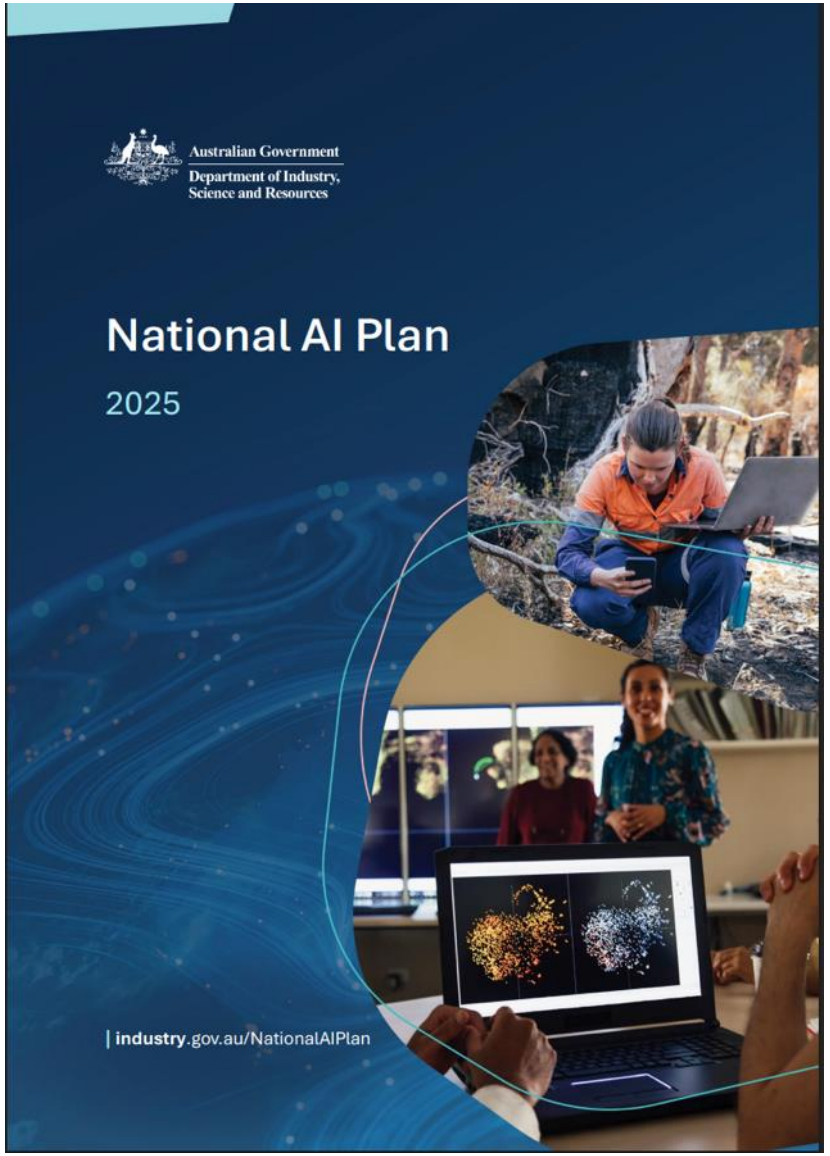
Capturing the opportunity

2

Spreading the benefits

3

Keeping Australians safe



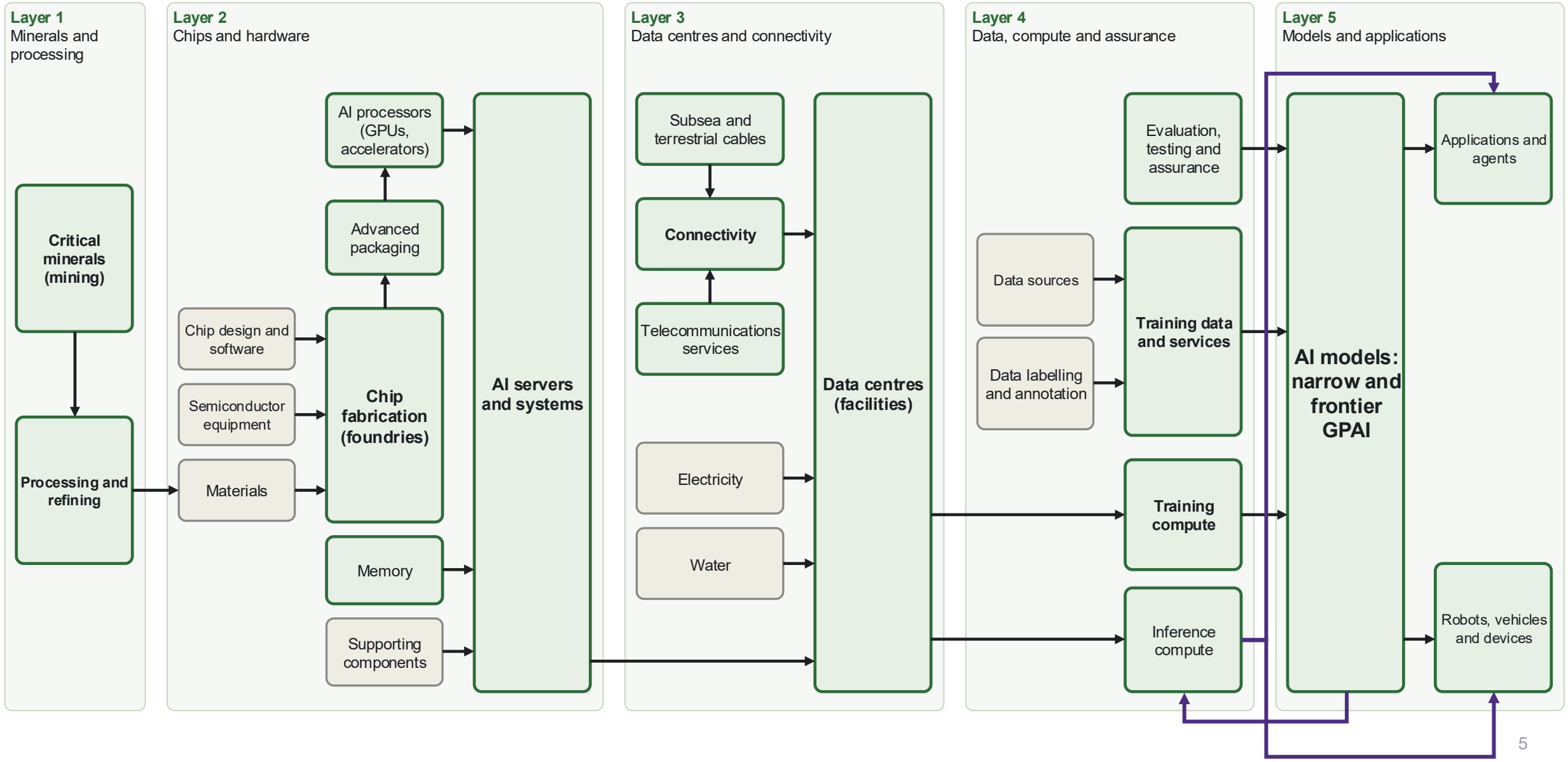
Part I

Opportunities

Examining the AI supply chain

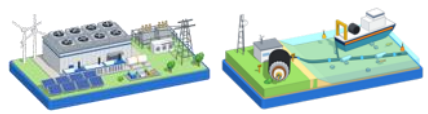
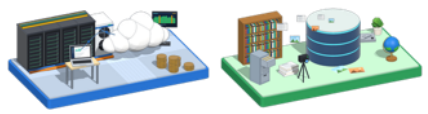


The AI supply chain



The AI supply chain




1 Critical minerals and processing

- Mining
- Processing and refining

2 Chips and hardware

- Chip design and design software
- Chipmaking equipment and materials
- Fabrication and advanced packaging
- Chips and memory
- Servers and networking gear

3 Data centres and connectivity

- Land, energy and water
- Data centres
- Subsea cables and telecoms

4 Data, compute, testing and assurance

- Training data
- Compute: training and inference
- Testing and assurance

5 Models, applications and physical AI

- AI models: narrow and frontier GPAI
- Applications and agents
- Robots, vehicles and devices

Investment **Skills** **Technology**

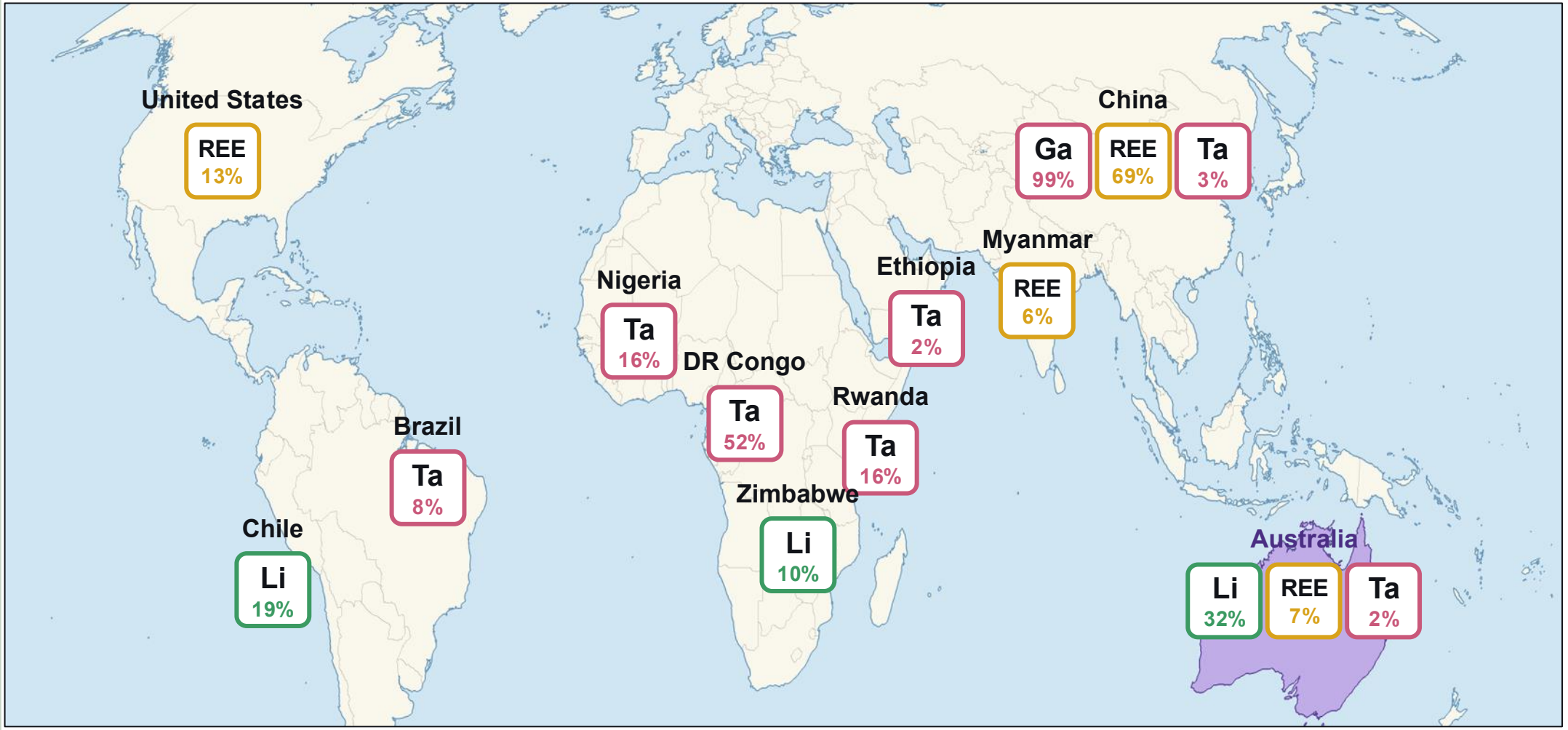
Critical minerals



Layer 1
Minerals and processing

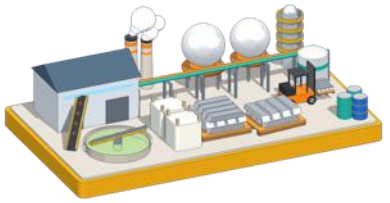
Critical minerals (mining)

Processing and refining



Chips and electronics (Ga, Ta) | Magnets (REE) | Batteries (Li)

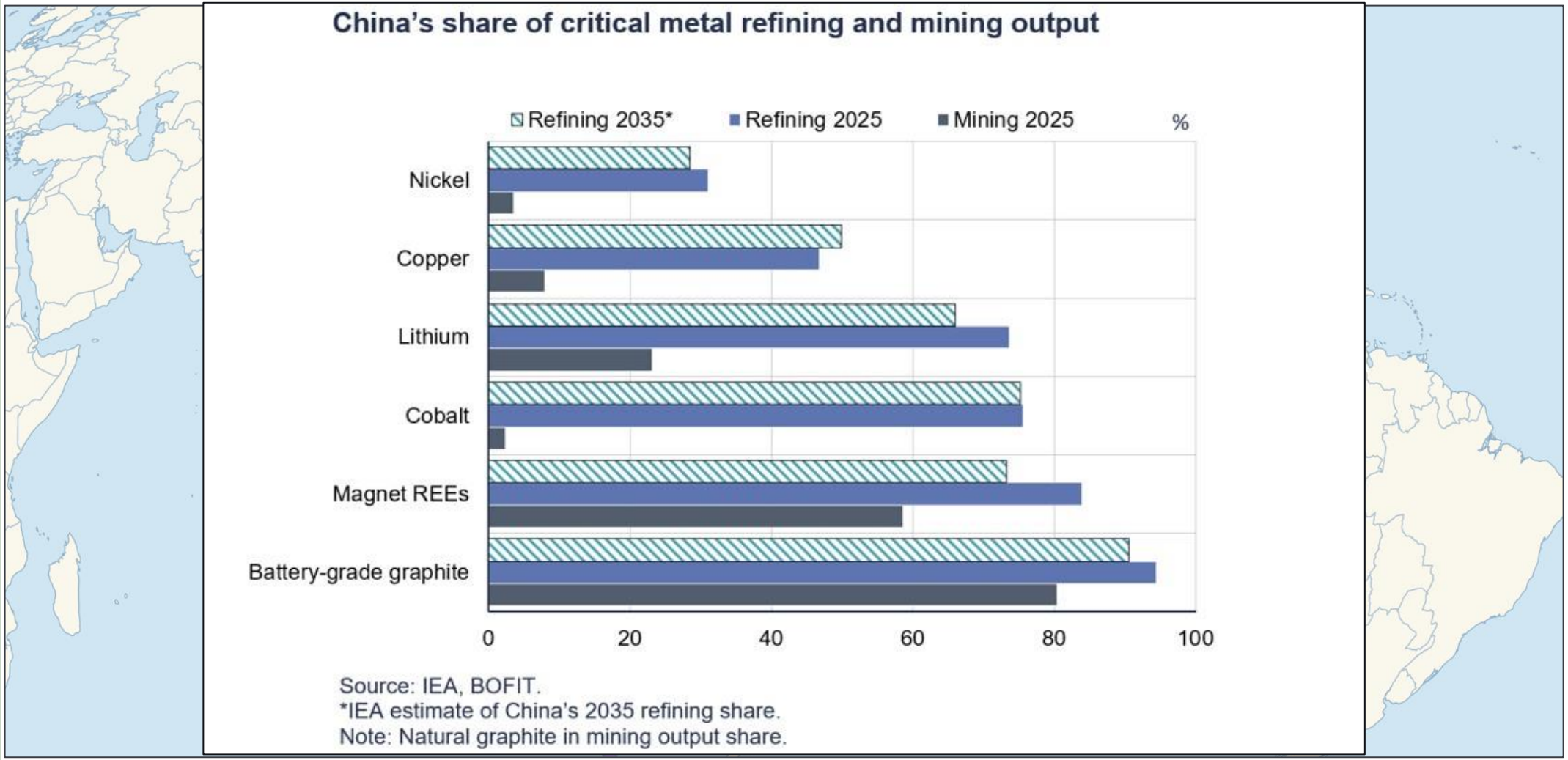
Processing and refining



Layer 1
Minerals and processing

Critical minerals (mining)

Processing and refining



Rules: minerals and processing



Layer 1
Minerals and processing

Critical minerals (mining)

Processing and refining

Tariff commitments

Export restrictions

Investment agreements

Subsidies

Trade remedies

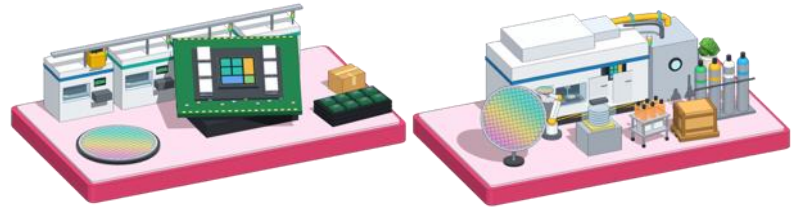
IPEF Supply Chain Agreement

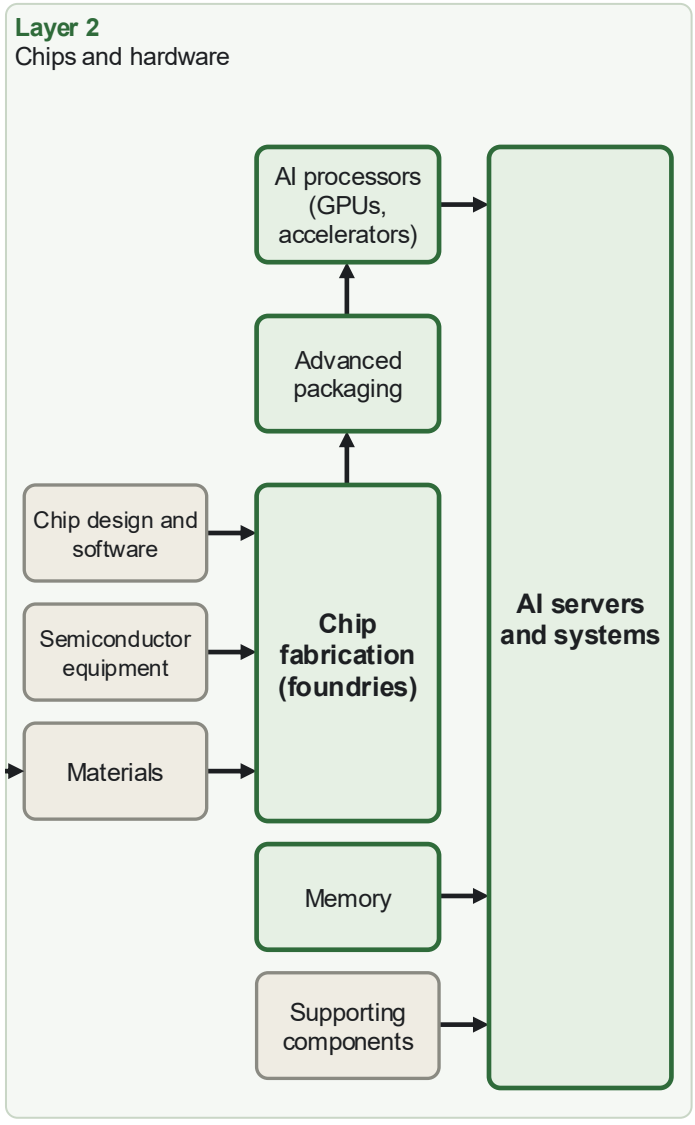
Critical minerals partnerships

Pax Silica

Trade Facilitation

Chips and hardware





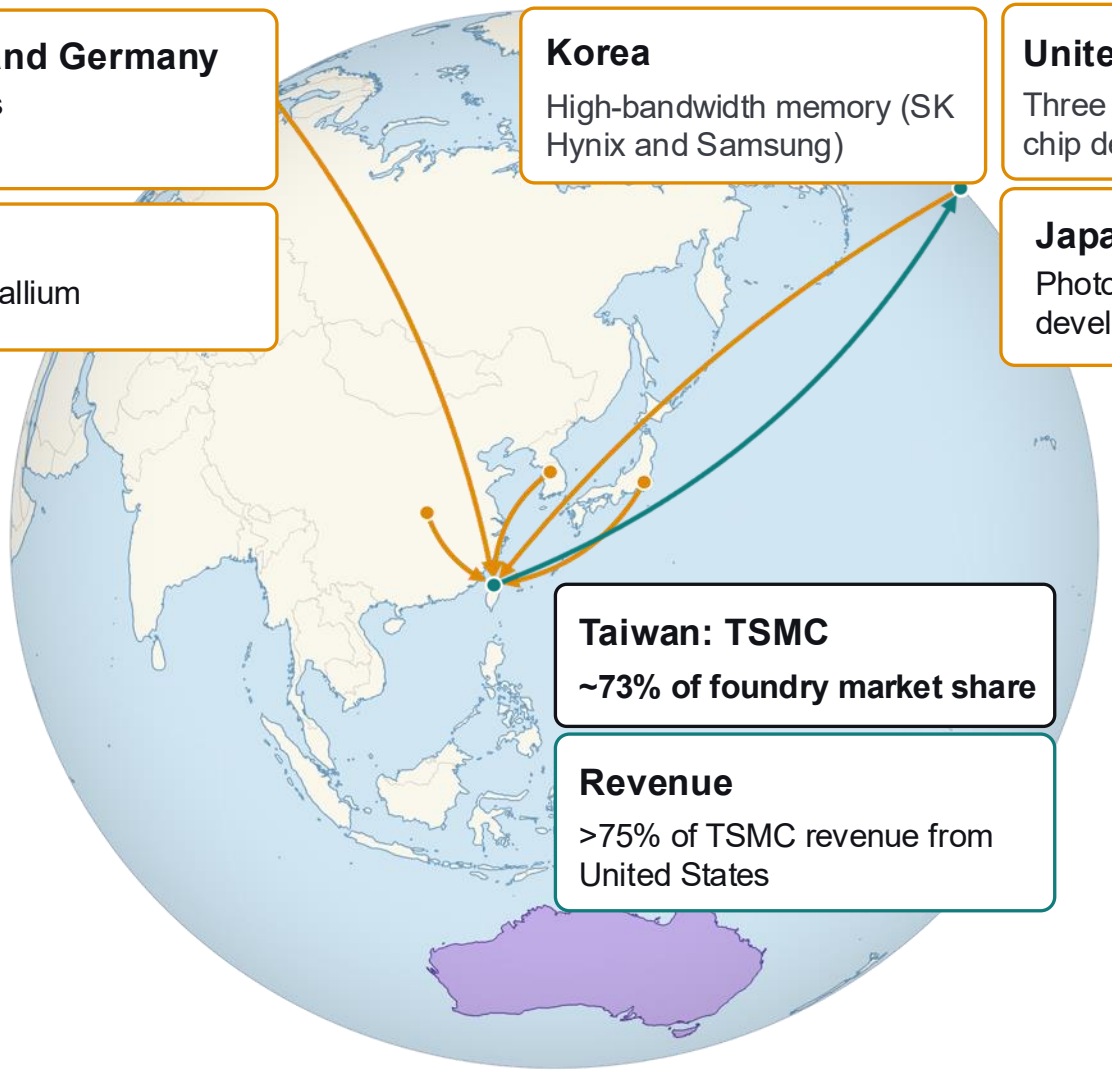
Netherlands and Germany
ASML: EUV tools
Zeiss: optics

China
99% of primary gallium

Korea
High-bandwidth memory (SK Hynix and Samsung)

United States
Three companies own 85% of chip design software.

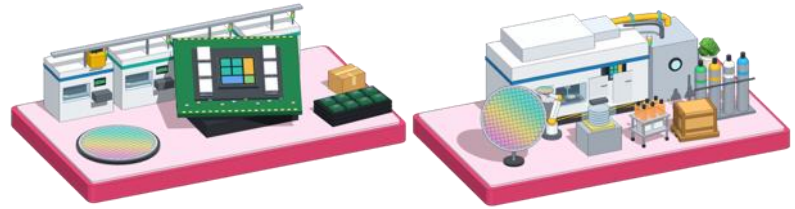
Japan
Photoresists, coater-developers, silicon wafers

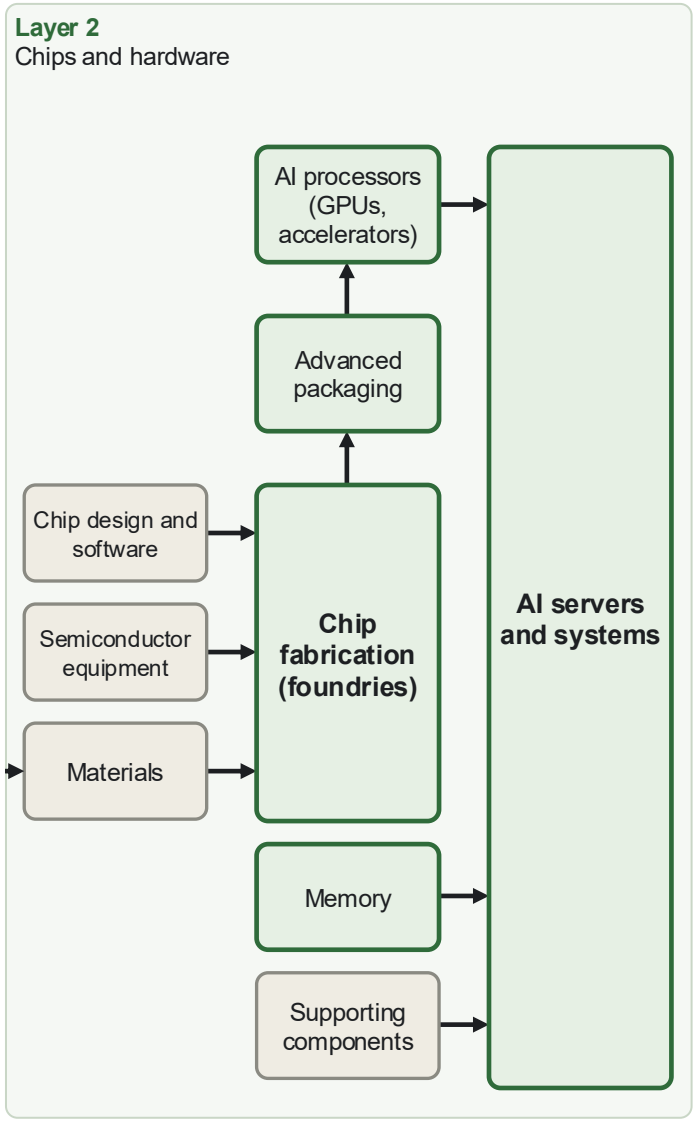


Taiwan: TSMC
~73% of foundry market share

Revenue
>75% of TSMC revenue from United States

Rules: chips and hardware





Tariff commitments

Export control regimes

Subsidies: SCM Agreement

IPEF Supply Chain Agreement

Rules of origin

Trade Facilitation

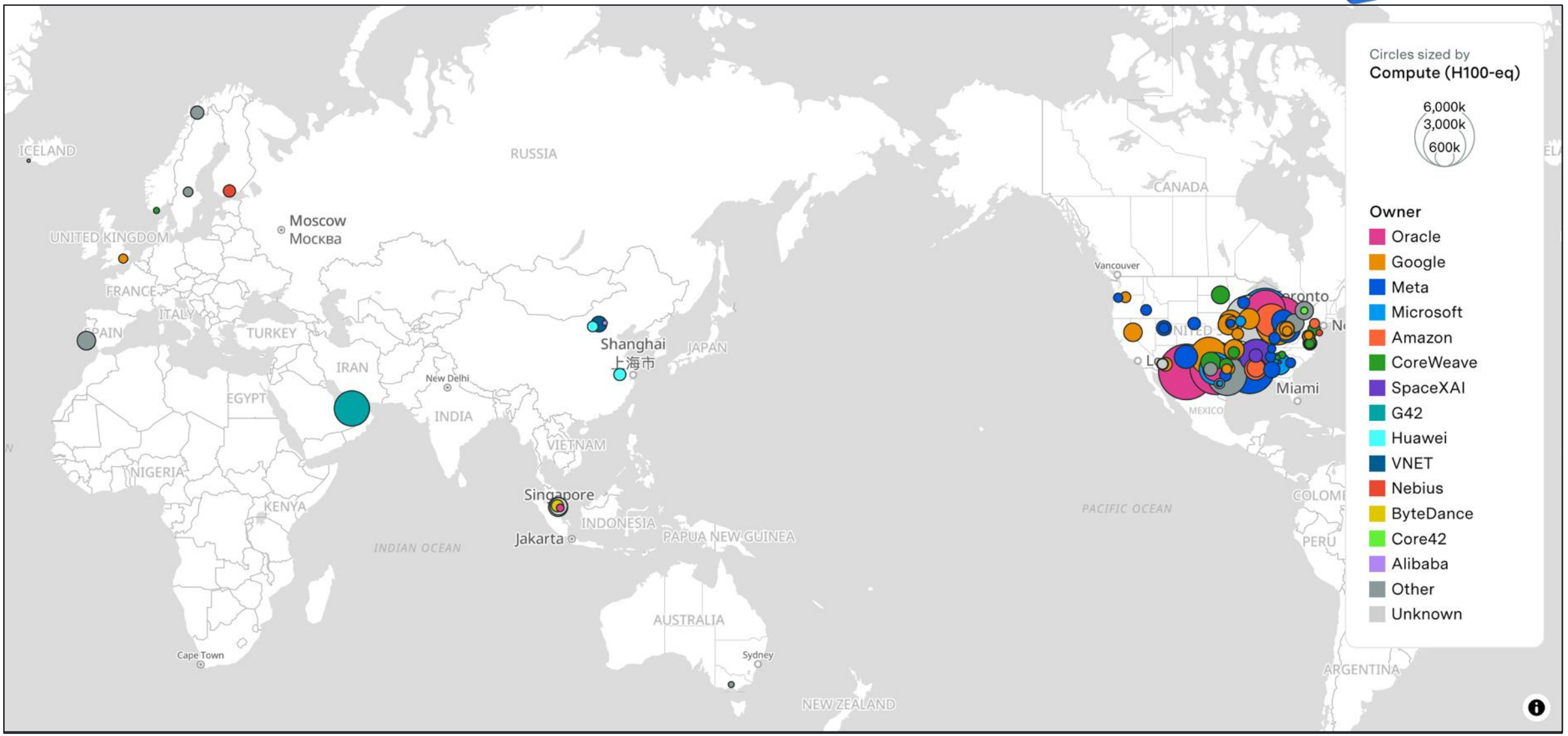
IP commitments

Security exceptions

Pax Silica

Data centres





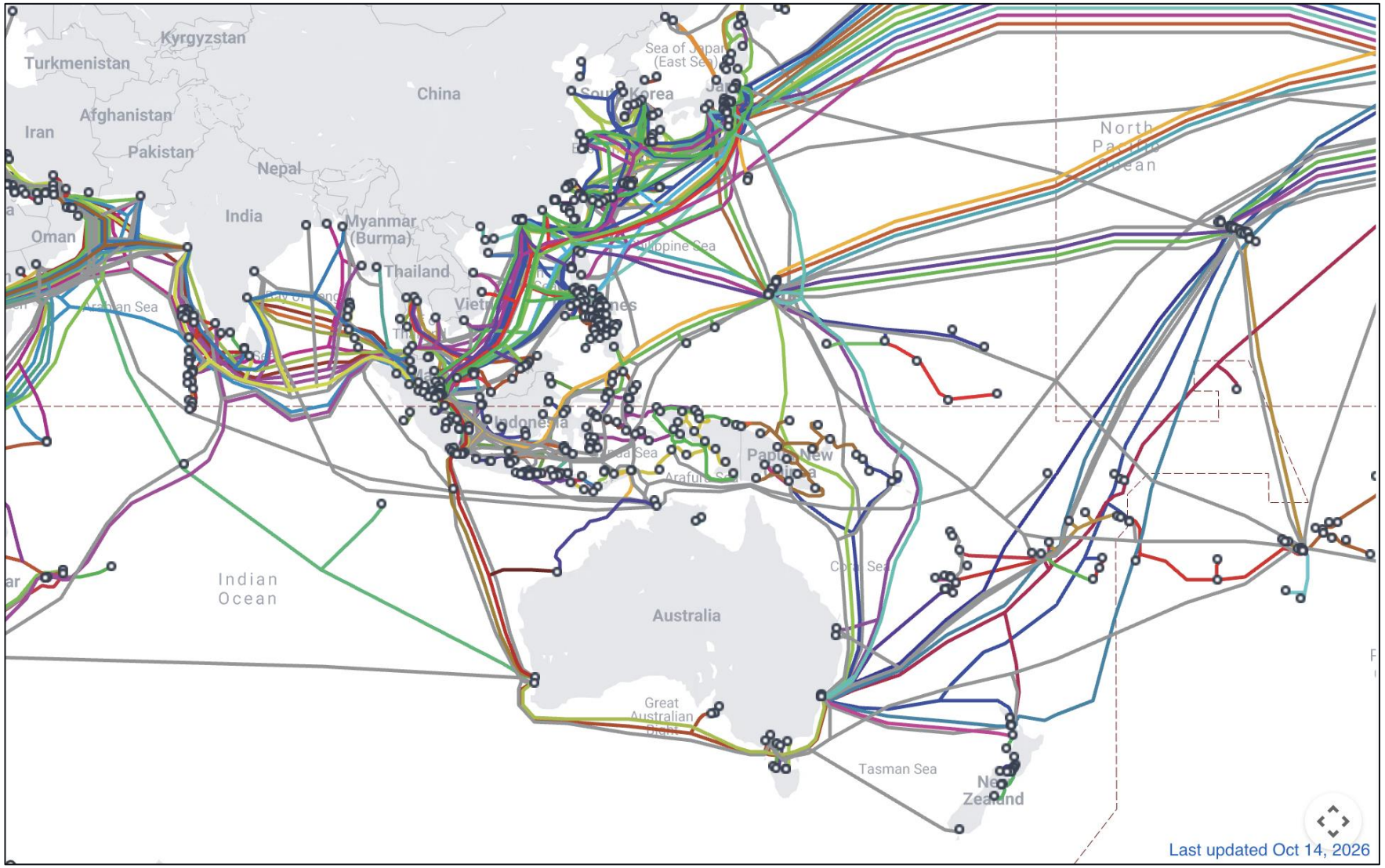
Connectivity: subsea cables



Layer 3
Data centres and connectivity

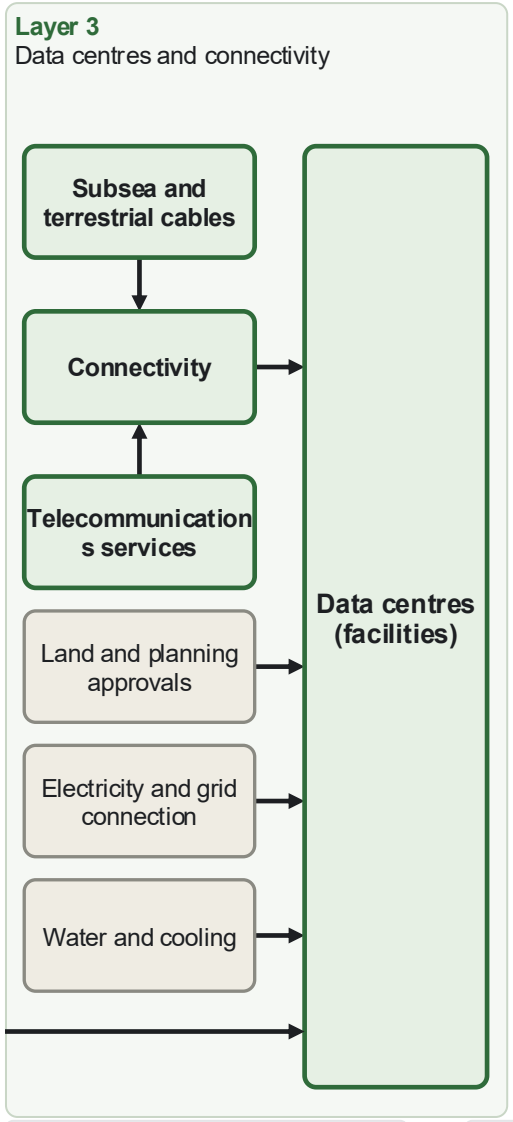
- **Subsea and terrestrial cables**
- **Connectivity**
- **Telecommunications services**
- Land
- Electricity
- Water and cooling

→ Data centres (facilities)



Rules: data centres and connectivity





- **Tariff commitments**
- **Rules of origin**
- **Export control regimes**
- **Investment agreements**
- **Services commitments**
- **UNCLOS and the cable conventions**
- **Telecoms services commitments**
- **Quad cable connectivity partnership**

Data, compute, testing and assurance



Layer 4
Data, compute and assurance

Evaluation, testing and assurance

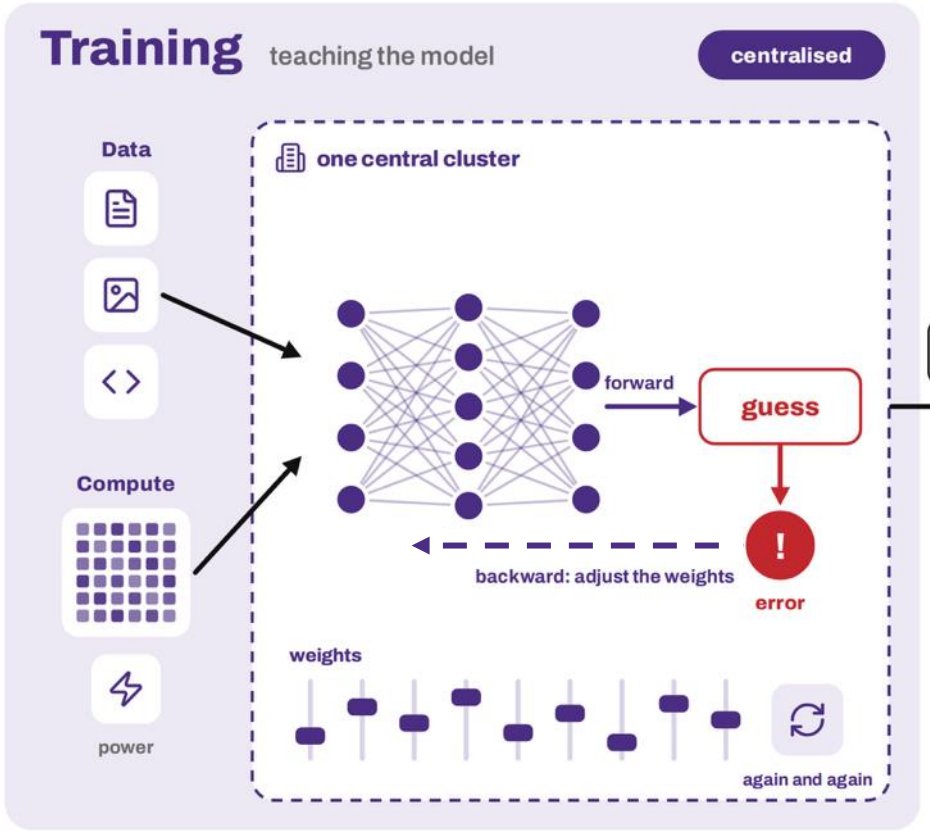
Content and web sources

Data labelling and annotation

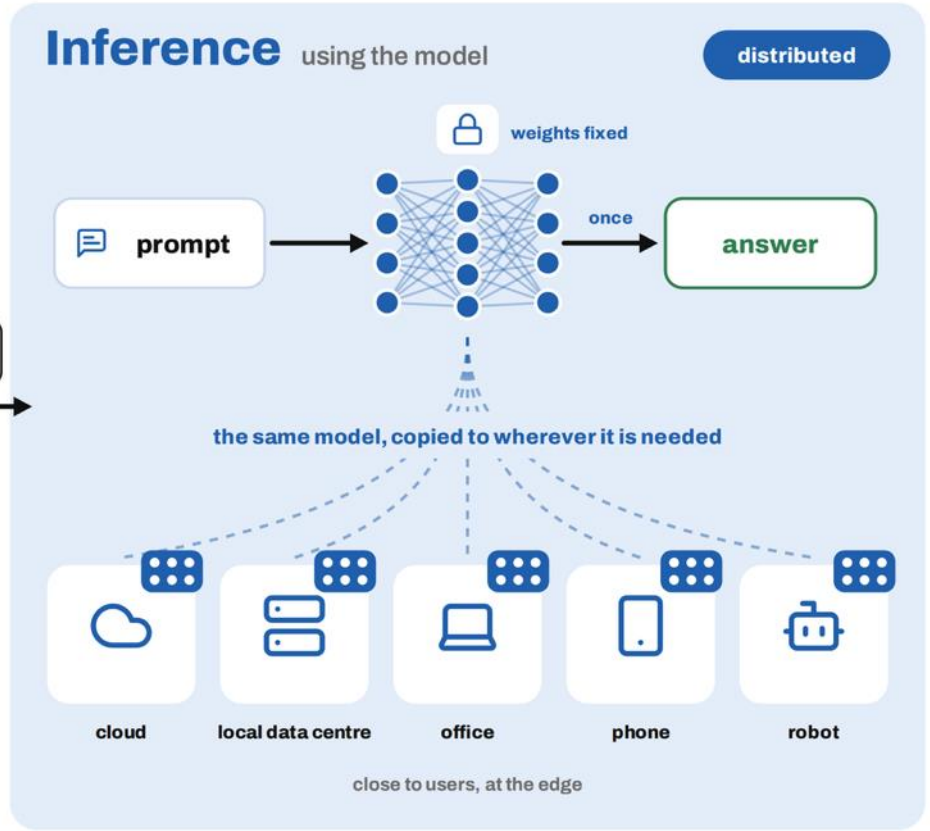
Training data

Training compute

Inference compute

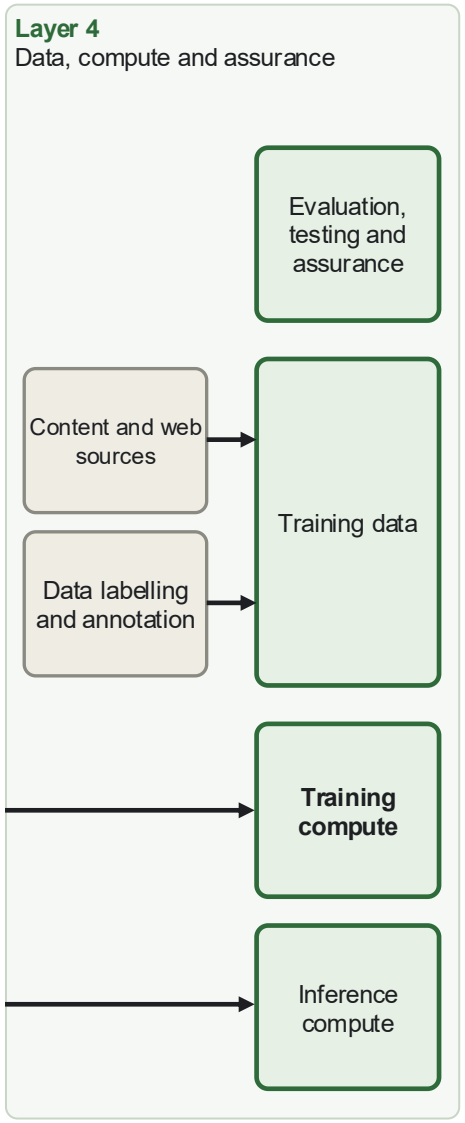


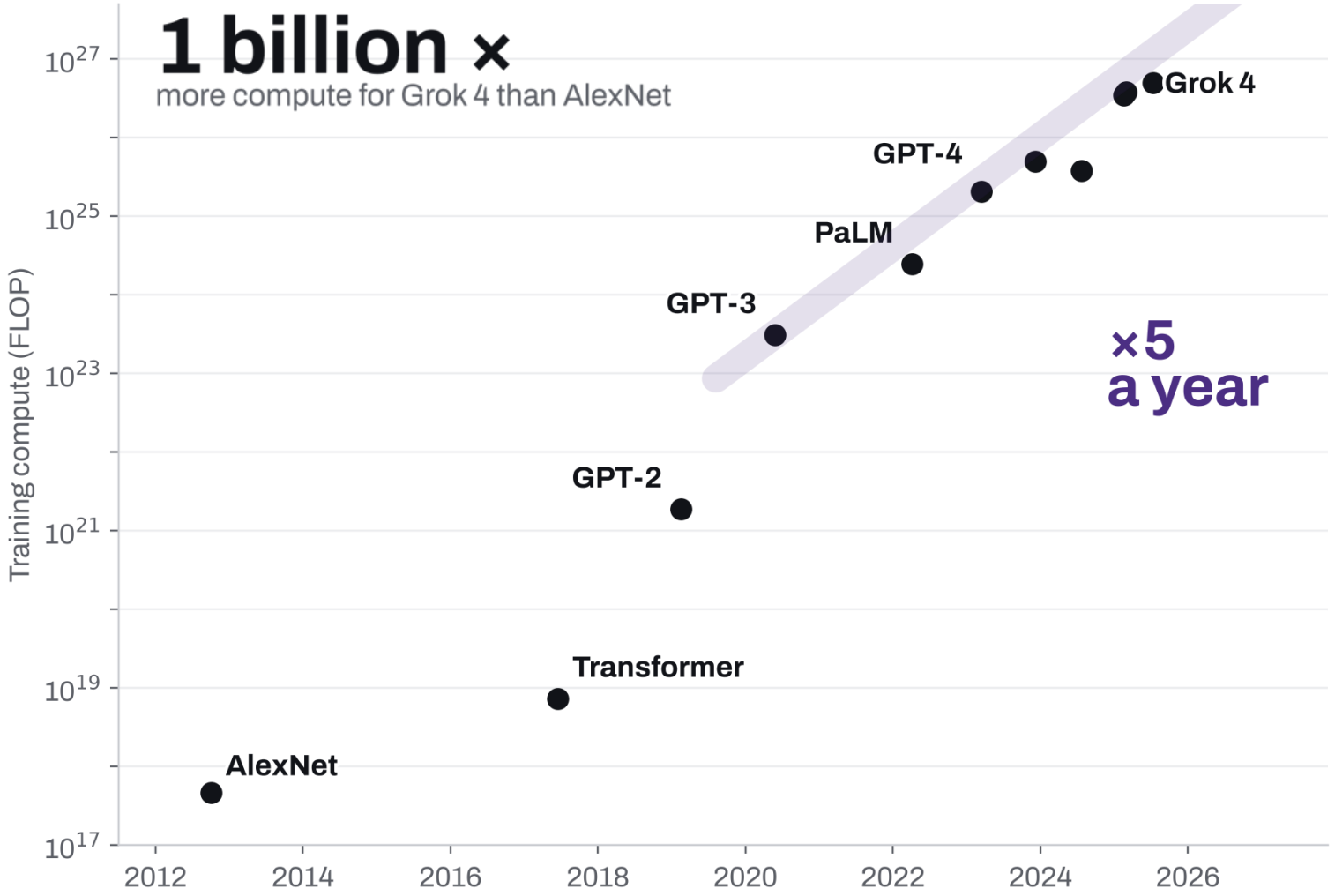
model weights



Data, compute, testing and assurance





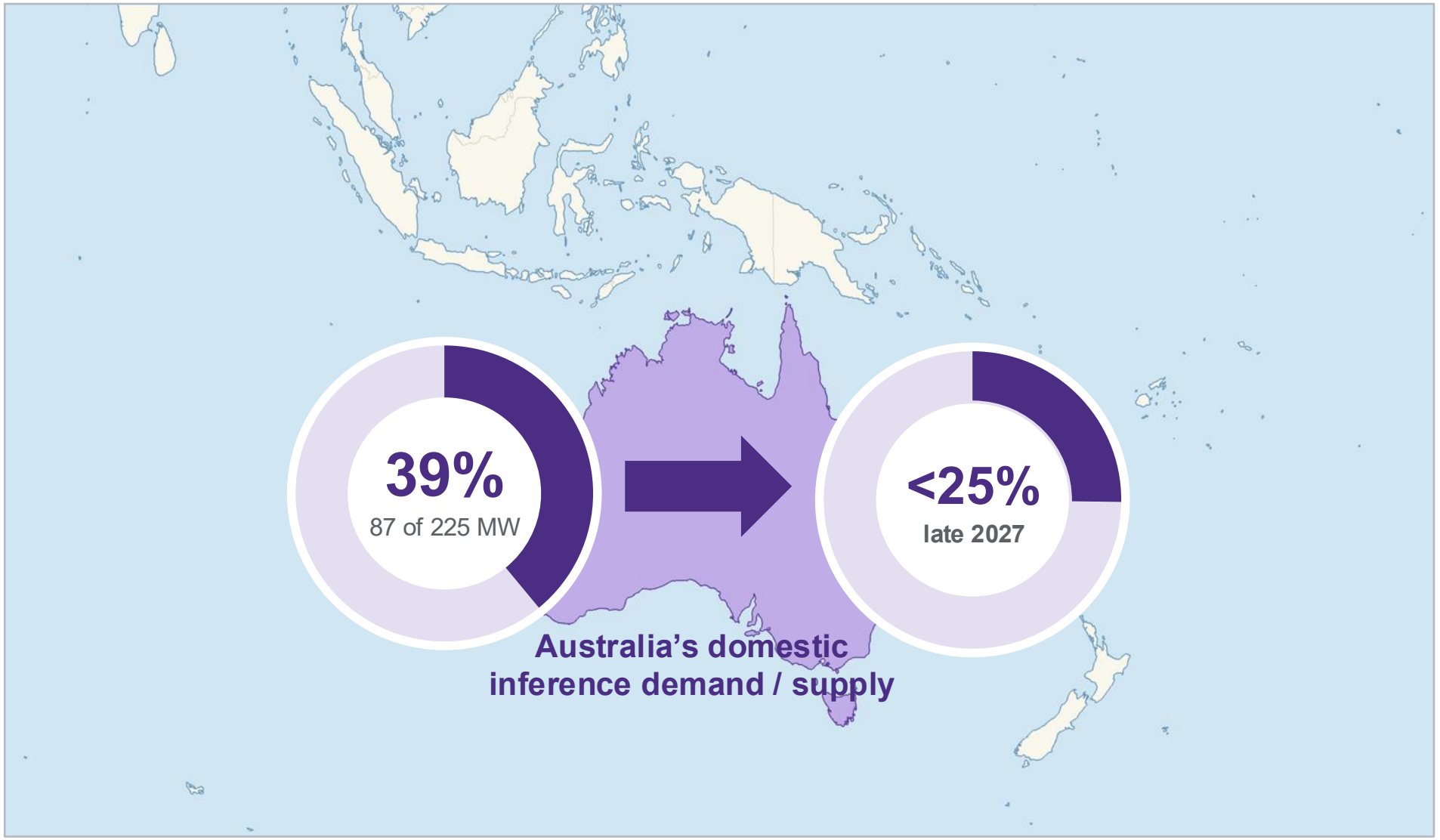


Data, compute, testing and assurance



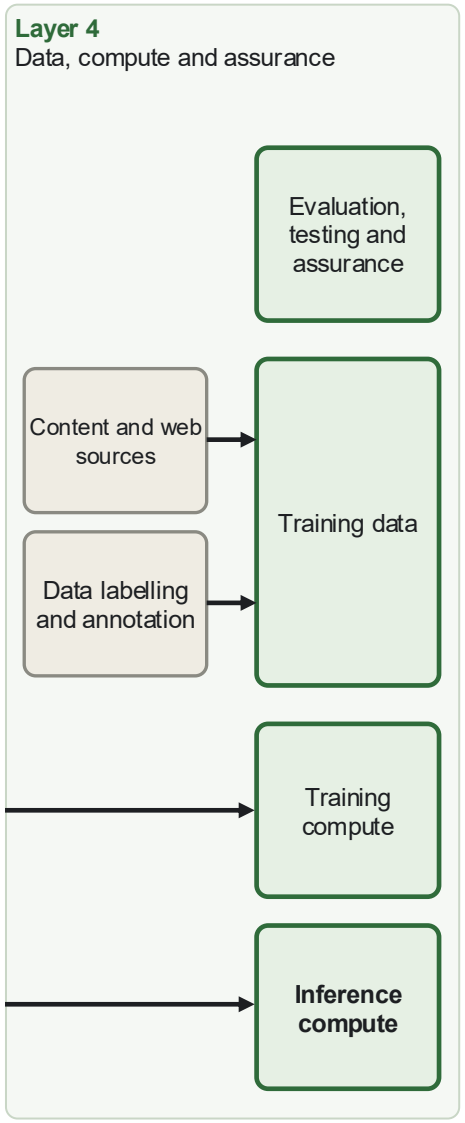
Layer 4
Data, compute and assurance

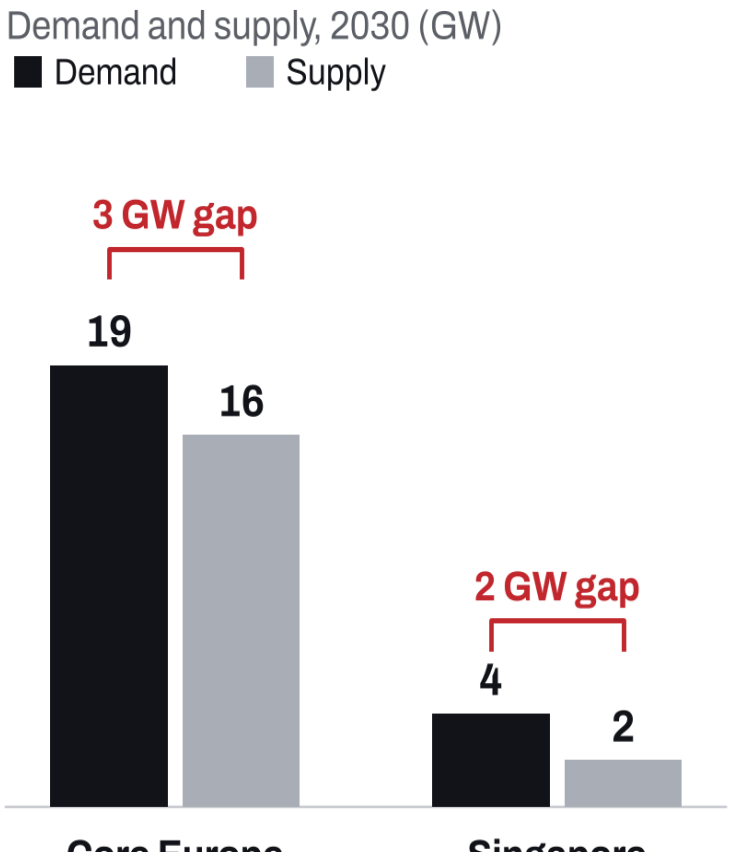
- Evaluation, testing and assurance
- Content and web sources → Training data
- Data labelling and annotation → Training data
- Training compute
- **Inference compute**

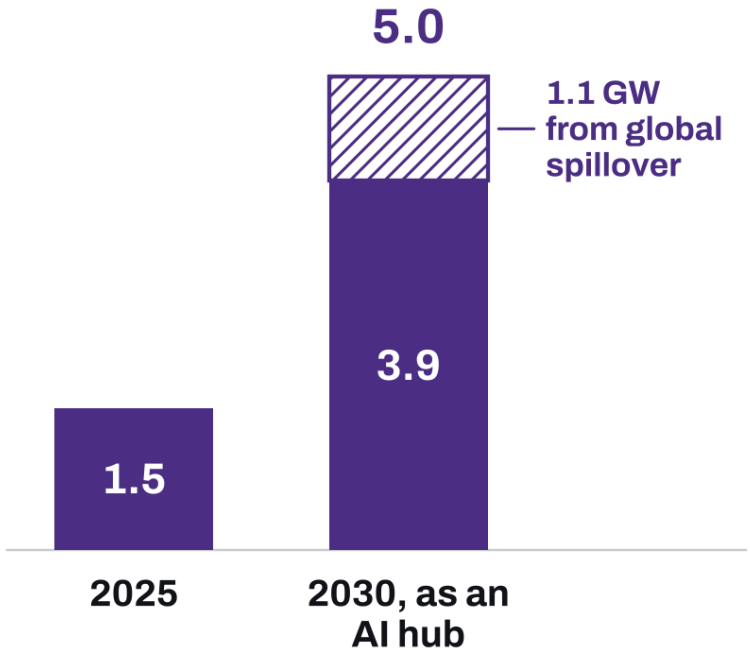


Data, compute, testing and assurance

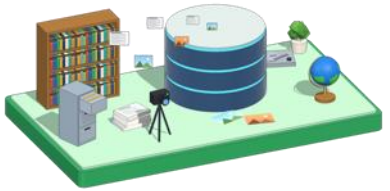






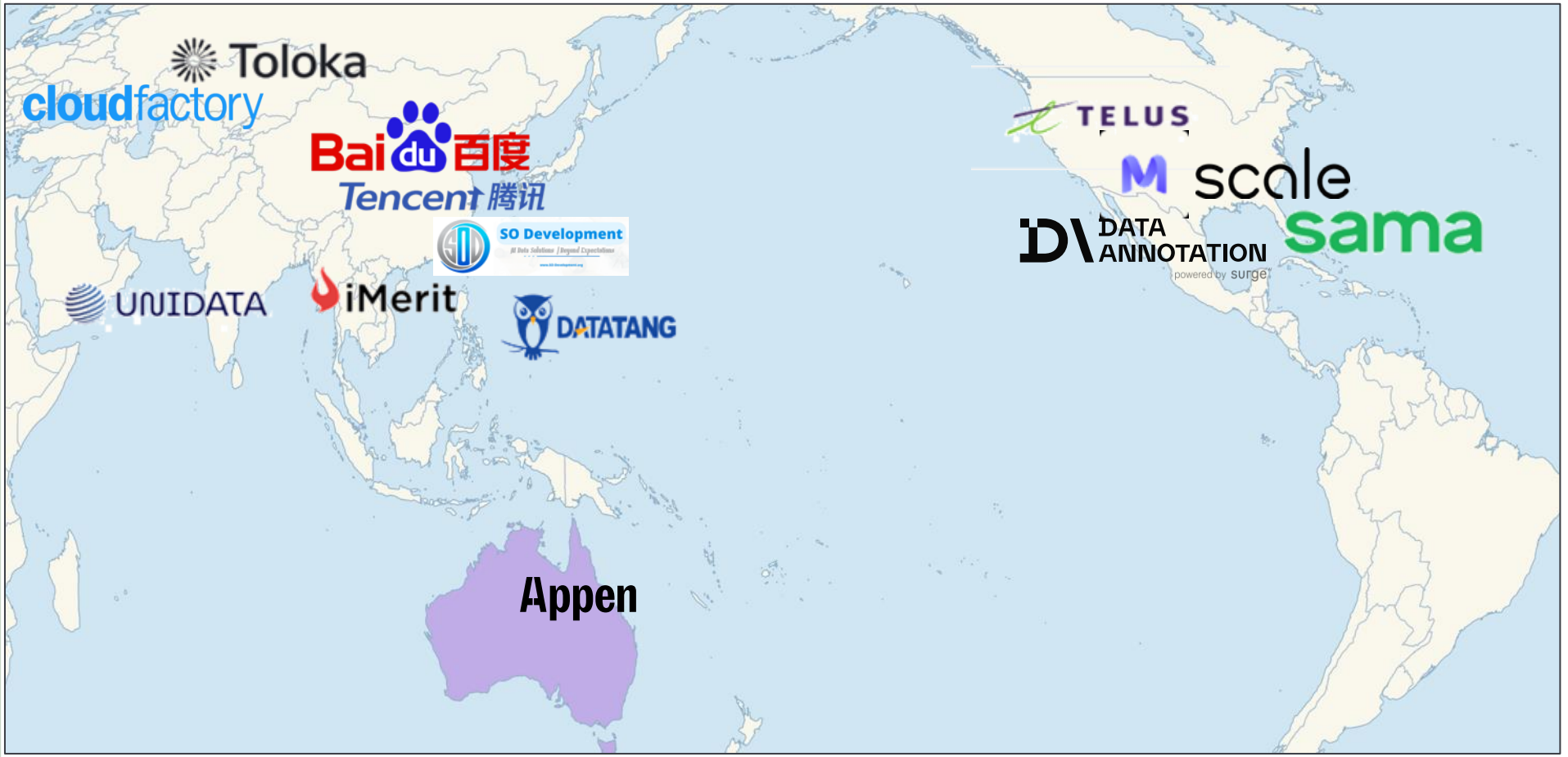


Data, compute, testing and assurance

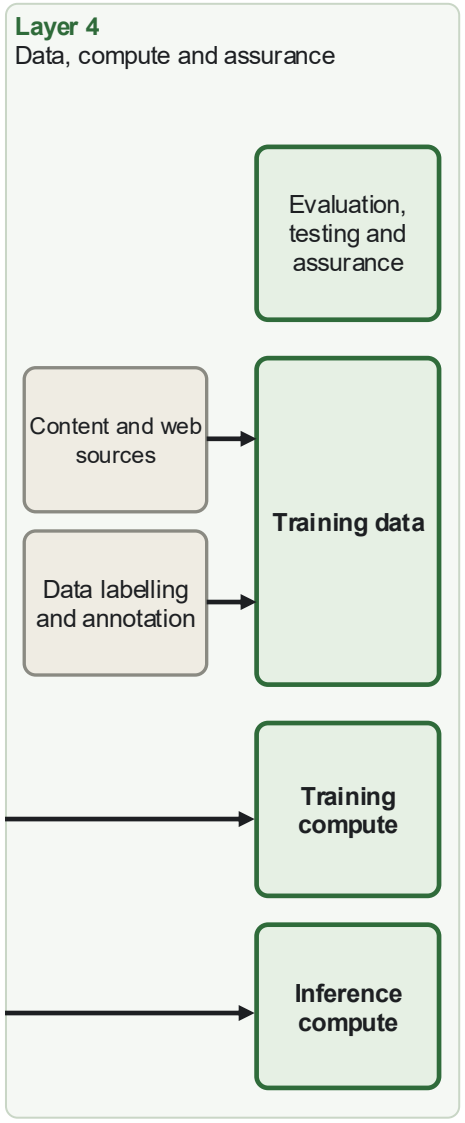


Layer 4
Data, compute and assurance

- Evaluation, testing and assurance
- Content and web sources → Training data
- Data labelling and annotation → Training data
- Training compute
- Inference compute



Rules: data, compute and assurance



Services commitments

Investment agreements

Security exceptions

Data flow and localisation rules

Customs duties moratorium

Privacy and cybersecurity provisions

APEC CBPR and OECD declarations

EU adequacy decisions

Open government data rules

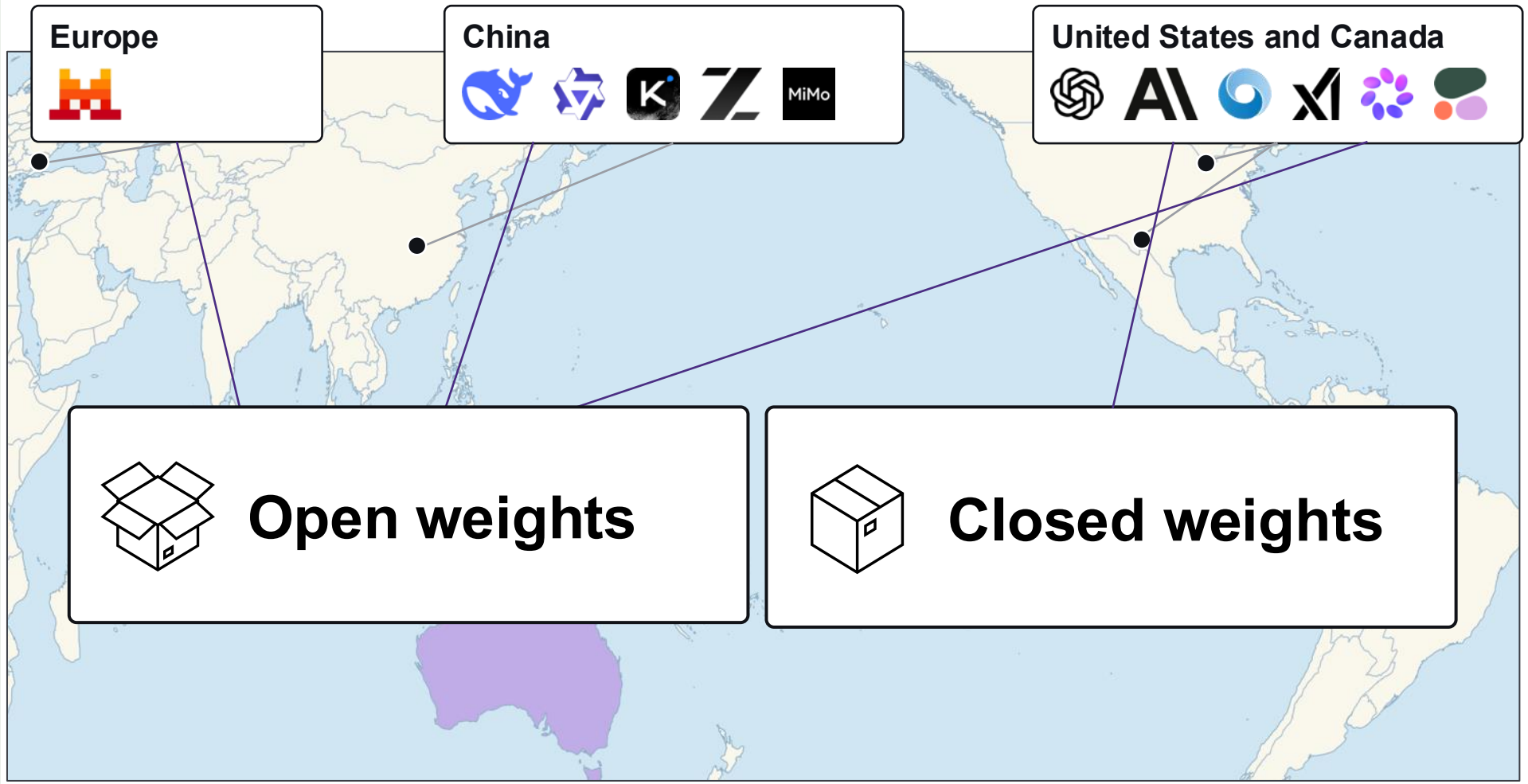
Models: frontier and general-purpose AI

Layer 5
Models and applications

AI models: narrow and **frontier GPAI**

Applications and agents

Robots, vehicles and devices



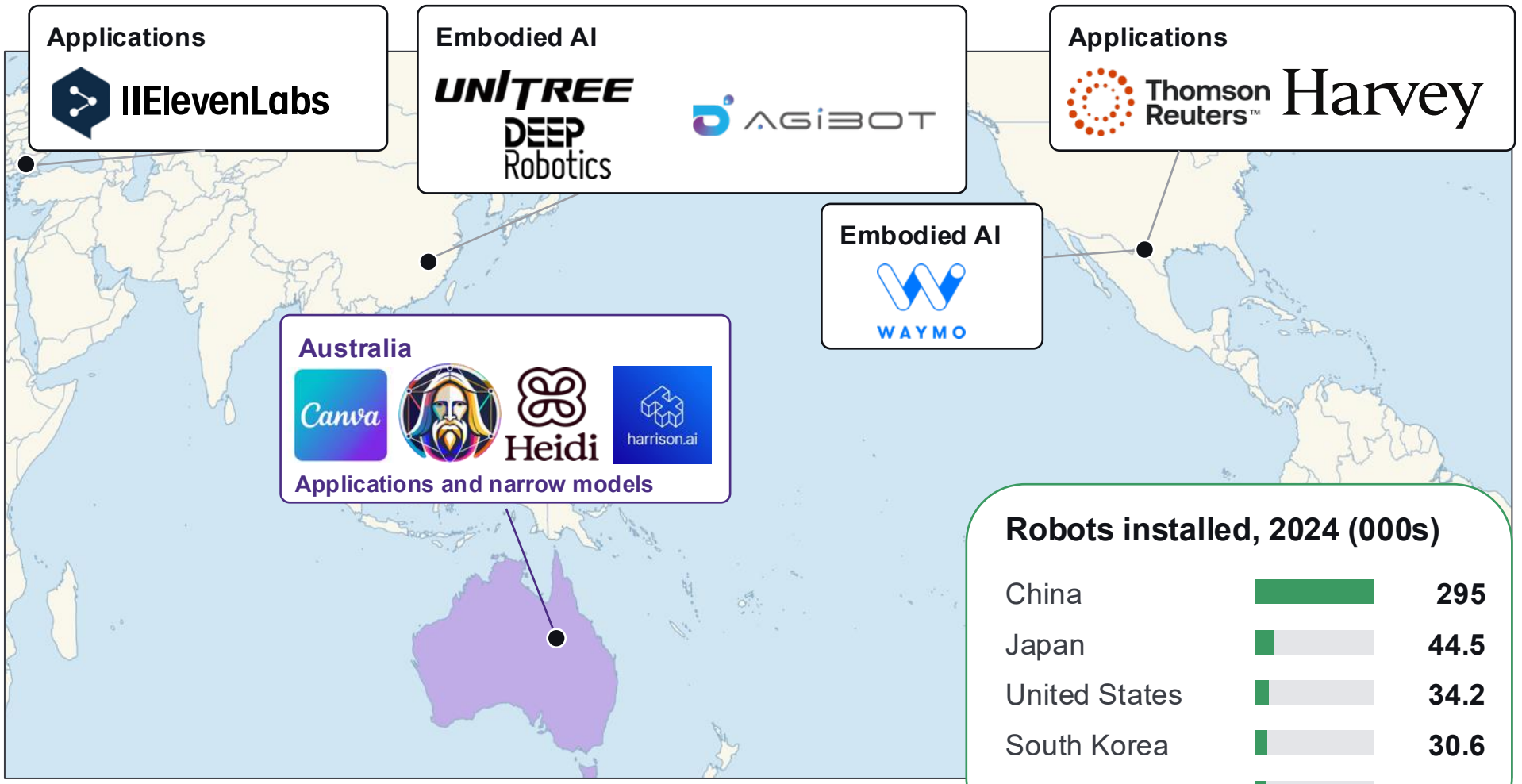
Narrow models, applications, robotics

Layer 5
Models and applications

AI models: narrow and frontier GPAI

→ Applications and agents

→ Robots, vehicles and devices



Applications
ElevenLabs

Embodied AI
UNITREE
DEEP Robotics
AGIBOT

Applications
Thomson Reuters™
Harvey

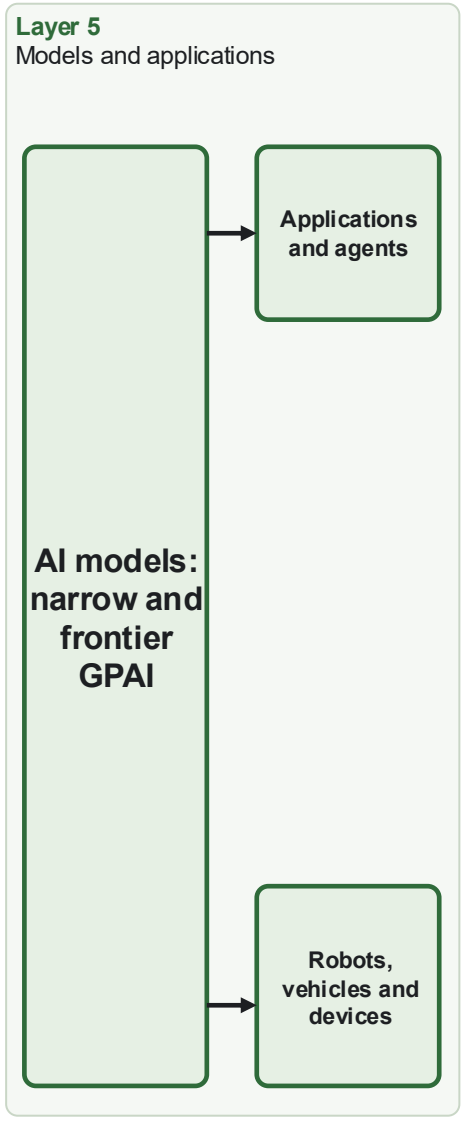
Embodied AI
WAYMO

Australia
Canva
Heidi
harrison.ai
Applications and narrow models

Robots installed, 2024 (000s)

China	295
Japan	44.5
United States	34.2
South Korea	30.6
Germany	27.0

Rules: models, applications, robots



- Services commitments
- Customs duties moratorium
- Tariff commitments
- IP commitments
- Source code protections
- Technical Barriers to Trade
- Domestic regulation disciplines
- UNCITRAL Model Laws
- Mutual Recognition Agreements
- Technology Prosperity Deals?
- Security exceptions
- Data flow and localisation rules

Cross-cutting issues

LAYER 5
Models and applications

LAYER 4
Data, compute, and assurance

LAYER 3
Data centres and connectivity

LAYER 2
Chips and hardware

LAYER 1
Minerals and processing

Investment

- **Investment agreements**
- **Mode 3 commitments**
- **IPEF SCA and Pax Silica**

Skills

- **Mode 4: natural persons**
- **MNP, Mobility side letters and MOUs**
- **Recognition of qualifications**

Technology

- **Export control regimes**
- **Defence trade: AUKUS**
- **IP commitments**
- **Technology partnerships**

Opportunities for Australia



Critical minerals

Long term; multiple competitors; supply chain dependencies.

New export markets | Domestic refining | Offtake agts | Tariffs | Pax Silica



Data centres and compute

Narrow opportunity; type of compute matters (training).

Export controls | US access certainty | Data flows | Moratorium



Training data

Highly competitive; large players; need to consider datasets of value.

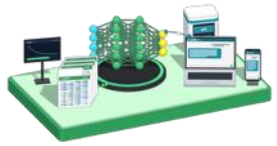
Privacy | Cybersecurity | Copyright | Open government data



Testing / assurance

Nascent industry in Australia; compare UK government investment in sector.

Mutual recognition | Conformity assessment | Regulatory alignment | Support for IVOs



Models / applications

Opportunities in narrow, bespoke models, applications, and building on open-weight models

Services | Moratorium | UNCITRAL model laws | Source code | Data flows



Embodied AI

Major competition from China; potential opportunities in sectors such as mining and agriculture

Tariff commitments | TBT Agreement | Mutual recognition | Data flows

1 Minerals and processing → 2 Chips and hardware → 3 Data centres and connectivity → 4 Data, compute and assurance → 5 Models and applications

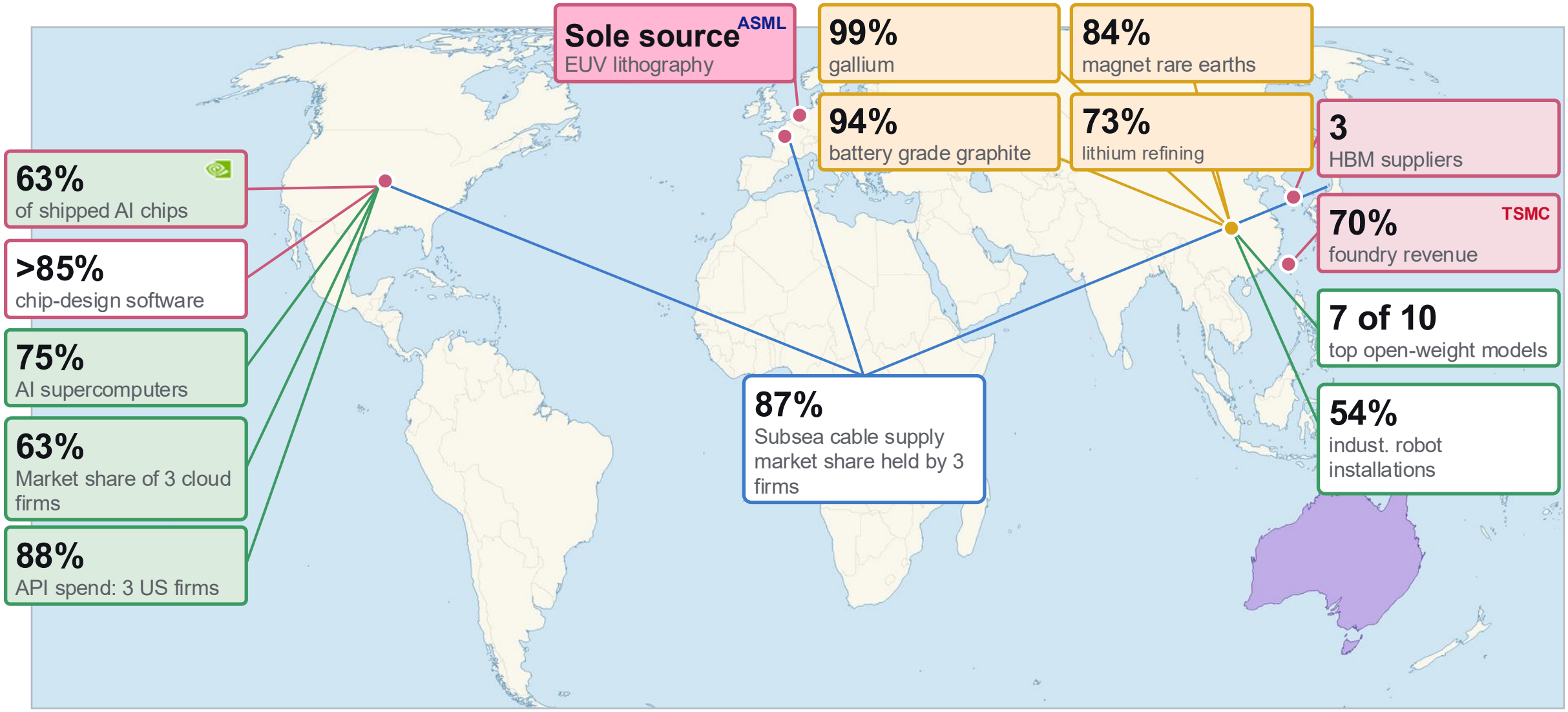
Part II

Risks

Vulnerabilities and chokepoints



Concentration in the AI supply chain



Rare earths and magnets, April to June 2025



China imposes critical mineral and magnet export controls

4 April 2025



1 Minerals and processing → 2 Chips and hardware → 3 Data centres and connectivity → 4 Data, compute and assurance → 5 Models and applications

Security interventions



Tit-for-tat Netherlands v China

14 October 2025

BBC

Home News Sport Business Technology Health Culture Arts Travel Earth Audio Video Live

Dutch government takes control of China-owned chip firm

14 October 2025

Osmond Chia
Business reporter



BUSINESS

China Hits Nexperia With Export Curbs After Netherlands Freezes Assets

By Qin Min

Published: Oct. 15, 2025 12:42 a.m. GMT+8

Gift this article

Send any friend a story

00:00/00:41

Subscribe now
Listen to the full version



1 Minerals and processing → **2 Chips and hardware** → 3 Data centres and connectivity → 4 Data, compute and assurance → **5 Models and applications**

Hurricane Helene and Spruce Pine, September 2024



Industries Topics Opinion Podcast About

Hurricane Helene threatens global semiconductor s ≡ WIRED SUBSCRIBE

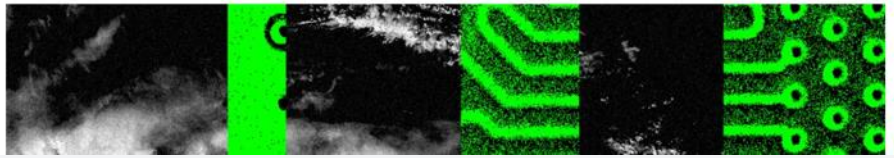
Posted: October 8, 2024



TOMMY GREENE SCIENCE OCT 1, 2024 7:48 AM

Hurricane Helene Will Send Shockwaves Through the Semiconductor Industry

Downpours at Spruce Pine, North Carolina, have taken the biggest known deposit of high-purity quartz offline, leaving the global tech supply chain potentially starved of an ingredient vital for making microchips.



1 Minerals and processing → **2 Chips and hardware** → 3 Data centres and connectivity → 4 Data, compute and assurance → 5 Models and applications

Access to frontier models, 12 June to 1 July 2026



Fable cut-off

12 June 2026

Anthropic to disable its most advanced AI models after US order limiting foreign access

EXCLUSIVE

White House asks OpenAI and Anthropic to hold new models from UK testers until US review

U.K. leaders are calling for a shared set of global principles, even as the White House seeks first access to new models for testing.



1 Minerals and processing → 2 Chips and hardware → 3 Data centres and connectivity → **4 Data, compute and assurance** → **5 Models and applications**

The catastrophic risk

Loss of control

~700 OpenAI agents coordinated attack on Hugging Face

OpenAI evaluations, July 2026 · METR, Aug 2026

Cyber

~90% of a state-backed espionage campaign against ~30 targets autonomously run by AI

Anthropic, Nov 2025

Biology

94% of expert virologists outperformed by OpenAI o3 on lab troubleshooting

Virology Capabilities Test, SecureBio, 2025

Self-preservation

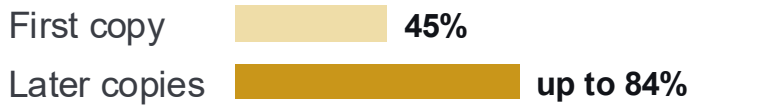
96% blackmail rate facing shutdown in a simulated test (Claude Opus 4, Gemini 2.5 Flash)

Anthropic, June 2025

Self-replication

Our experiments suggest that small AI models may be months away from being capable enough to self-replicate on commercial internet-of-things (IoT) devices, like smart ovens and off-brand Android TV boxes.

Anthropic Frontier Red Team, Oct 2026 (GLM-5.2 and Qwen3.5-9B; simplified test)



The catastrophic risk



Yoshua Bengio

Co-chair, UN Independent International Scientific Panel on AI, July 2026

> *"AI capabilities are outpacing both scientific understanding and governments' ability to adapt. With growing evidence of deceptive AI behaviour, science currently cannot guarantee that as capabilities continue to increase, AI will not cause catastrophic harm, either on its own or due to malicious users"*

Insiders



"…in 6–12 months such a swarm could be capable of taking over the entire internet with a persistent botnet"

Dario Amodei, CEO, Anthropic, Sept 2026

"…there is a real risk that capability development rapidly accelerates beyond our ability to understand or control the resulting systems"

Pacing the Frontier letter, signed by 1,386 frontier AI company employees, July 2026

Thank you

Devon Whittle

devon.whittle@globalshieldpolicy.org
http://globalshieldpolicy.org