How **geopolitics** is rerouting **submarine cables...**

nodal/ys

Jocelinn Kang
AusNOG 2025

Once upon a time...

Once upon a time...

- Dominated by telcos
  - Driven by market-demand
  - Straightest, most direct route
  - To population centres

- But now...
  - Two major influences are shaping the subcables industry and the global subcables network...

Hyperscalers & geostrategic competition

“The Influencers”

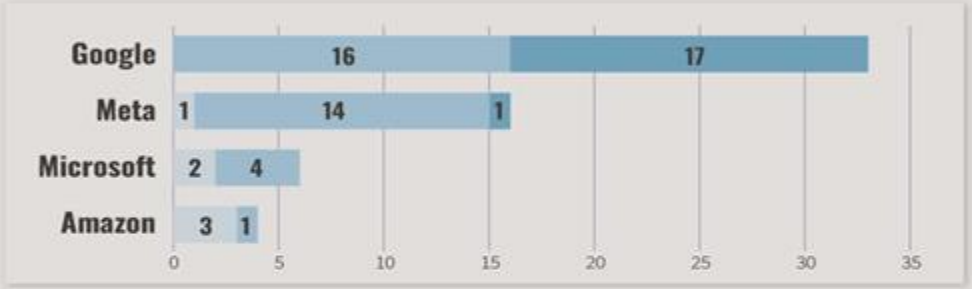
Hyperscaler investment in cables

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*)

As at September 2024

Acronyms

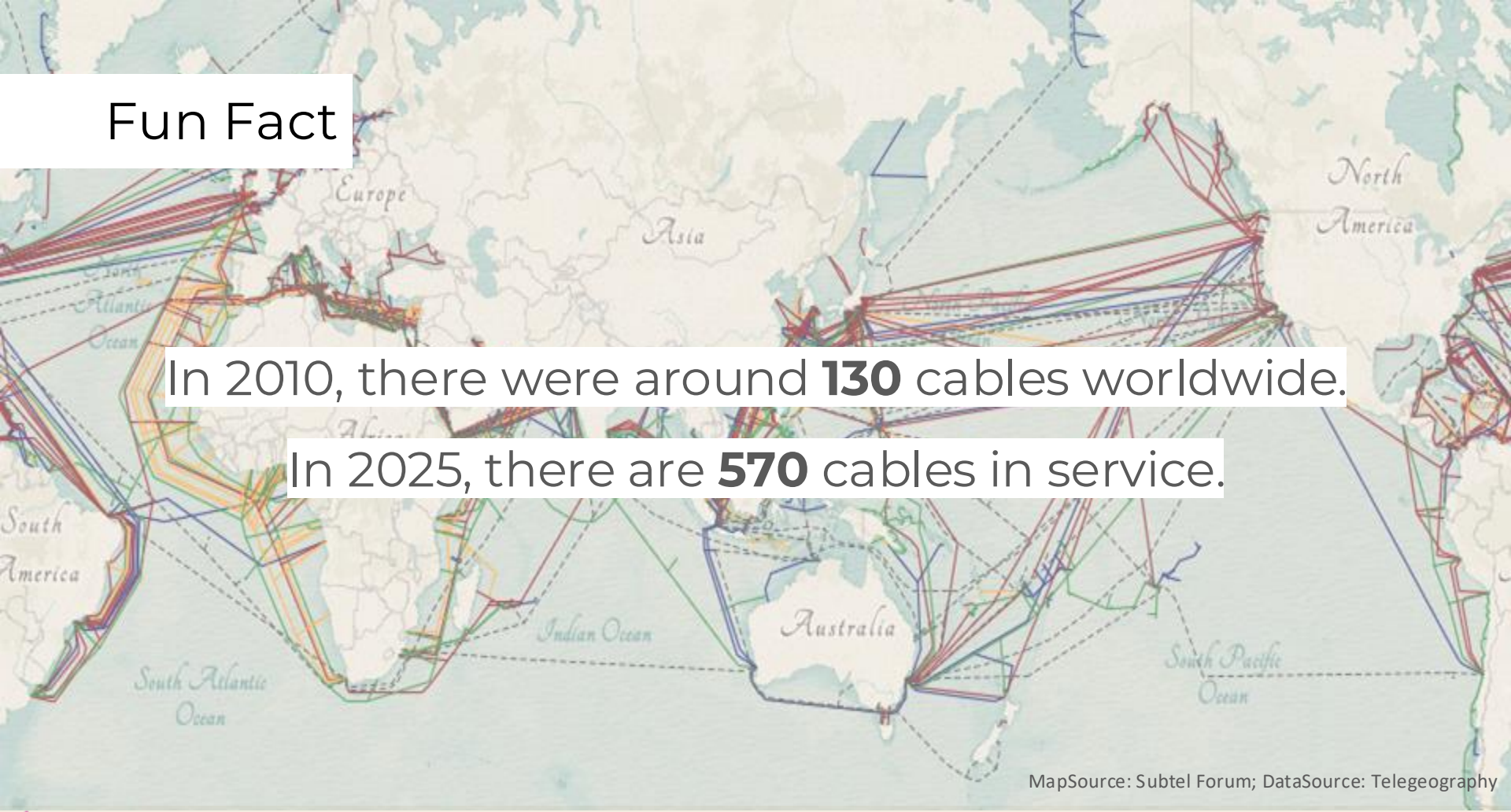
SJC	Southeast Asia-Japan Cable
AEC-1	America Europe Connect
APG	Asia Pacific Gateway
NCP	New Cross Pacific Cable System
JGA-S	Japan-Guam-Australia South
PLCN	Pacific Light Cable Network
H/CC-2	Havhingsten/CeltixConnect-2
H/NSC	Havhingsten/North Sea Connect
SJC2	Southeast Asia-Japan Cable 2
NPCI	North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



Hyperscalers

- Connecting data centres instead of population centres
- Four hyperscalers, Google, Meta, AWS and Microsoft account for >70% of global subcable bandwidth usage (2023)!
- By comparison in 2016, majority of demand came from internet backbone providers
- Vertical integration
- Affecting supply chains

Fun Fact



In 2010, there were around **130** cables worldwide.

In 2025, there are **570** cables in service.

MapSource: Subtel Forum; DataSource: Telegeography

Why are submarine cables strategic assets?

- They facilitate communication, trade, finance...
- They carry more than data -- sovereignty, the modern digital economy, enabler of future-technology (eg. AI).
- Control of cable systems means power.

→ **economic power and information advantage**

National resilience

- **Network resilience vs National resilience**
  - Network resilience is about uptime; National resilience is about keeping the systems we rely on running, even during crises.
- **Self-sufficiency:** Governments are worried about relying on cable systems built or maintained by geopolitical rivals.
- **National security questions**:

  Who built it? Where does it land? Who can disrupt it? Who can access the data?

Instruments of geopolitical influence

- Use of **diplomatic and political pressure** to create **exclusion from supply chains.** Response: Attempting to create self-sufficiency in supply chains.
- Leveraging **laws and regulations**:
  - Permits - For cables that go through the South China Sea, increasingly difficult to get Chinese permits for cable deployment. Installers responding by avoiding SCS; Repairs in contested areas.
  - Licenses - US opposed to cables that connect US with China mainland or Hong Kong. Operators respond by connecting to SEA and Australia.

Effects on the industry and global subcable network

Connectivity & Resilience

- Which countries are directly connected together
- Cable routes (not always the most direct route)
- Cables landing location*

Costs

- Permits, licenses and project schedules

Supply Chain

- Which companies can be involved in which systems & repairs
- Which company's equipment are used in a cable system
- Access to cable laying vessels*

* Also hyperscalers

Geostrategic competition in action

Case Studies

US vs China

- Pacific Light Cable Network (PLCN)
- BtoBE → CAP-1
- SEA-ME-WE6
- Southeast Asia-Japan 2 (SJC2)

Source: Image created by the authors, using cable data from *TeleGeography*.

To the US →

Chinese self-sufficiency in the subsea cable supply chain

(Key Chinese players in critical sectors of the subsea cable market)

	Chinese companies	Global rivals
Main investors	China Telecom, China Mobile, China Unicom	Google (U.S.), Amazon (U.S.), Meta (U.S.)
Cable builders, equipment suppliers	HMN Technologies, FiberHome	SubCom (U.S.), Alcatel Submarine Networks (France), NEC (Japan)
Fiber optic cables	Hengtong, FiberHome, Yangtze Optical Fibre and Cable, Jiangsu Zhongtian Technology	Corning (U.S.), Nexans (France), NEC (Japan), Furukawa Electric (Japan)
Optical components, chips	Wuhan Fisilink Microelectronics Technology, Huawei Technologies, Zhongji InnoLight, Accelink Technologies	Broadcom (U.S.), Coherent (U.S.), Sumitomo Electric Industries (Japan)
Repeaters	HMN Tech, FiberHome	NEC (Japan), SubCom (U.S.)
Cable ship operators	FiberHome Marine, China Submarine Cable Construction*, S.B. Submarine Systems	TE SubCom (U.S.), Global Marine Group (U.K.), LDA Group (France)
Data center, server makers	Huawei, Inspur, Lenovo	Google (U.S.), Meta (U.S.), Amazon (U.S.)

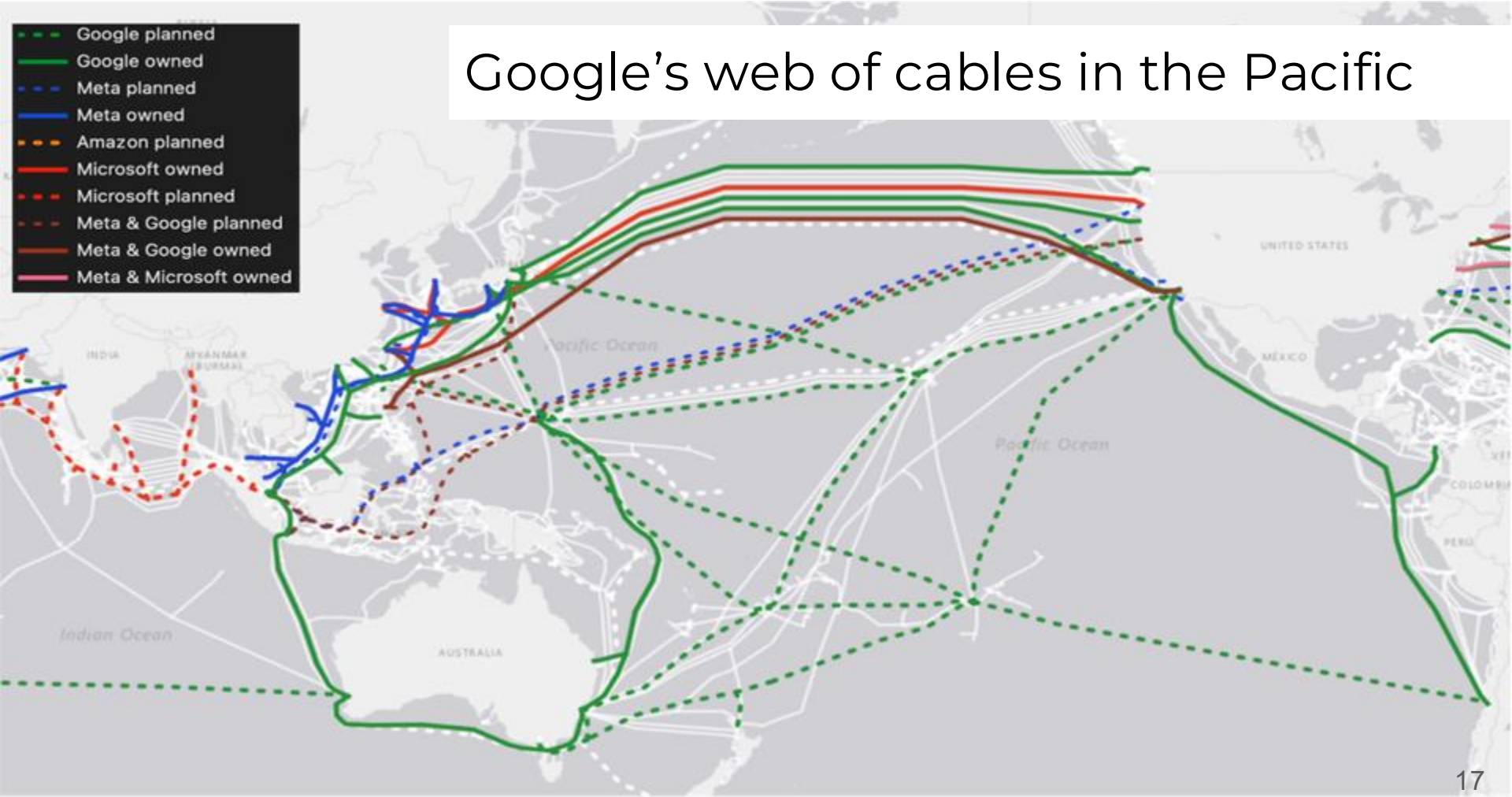
**Subsidiary of China Telecom*

Source: Nikkei Asia research

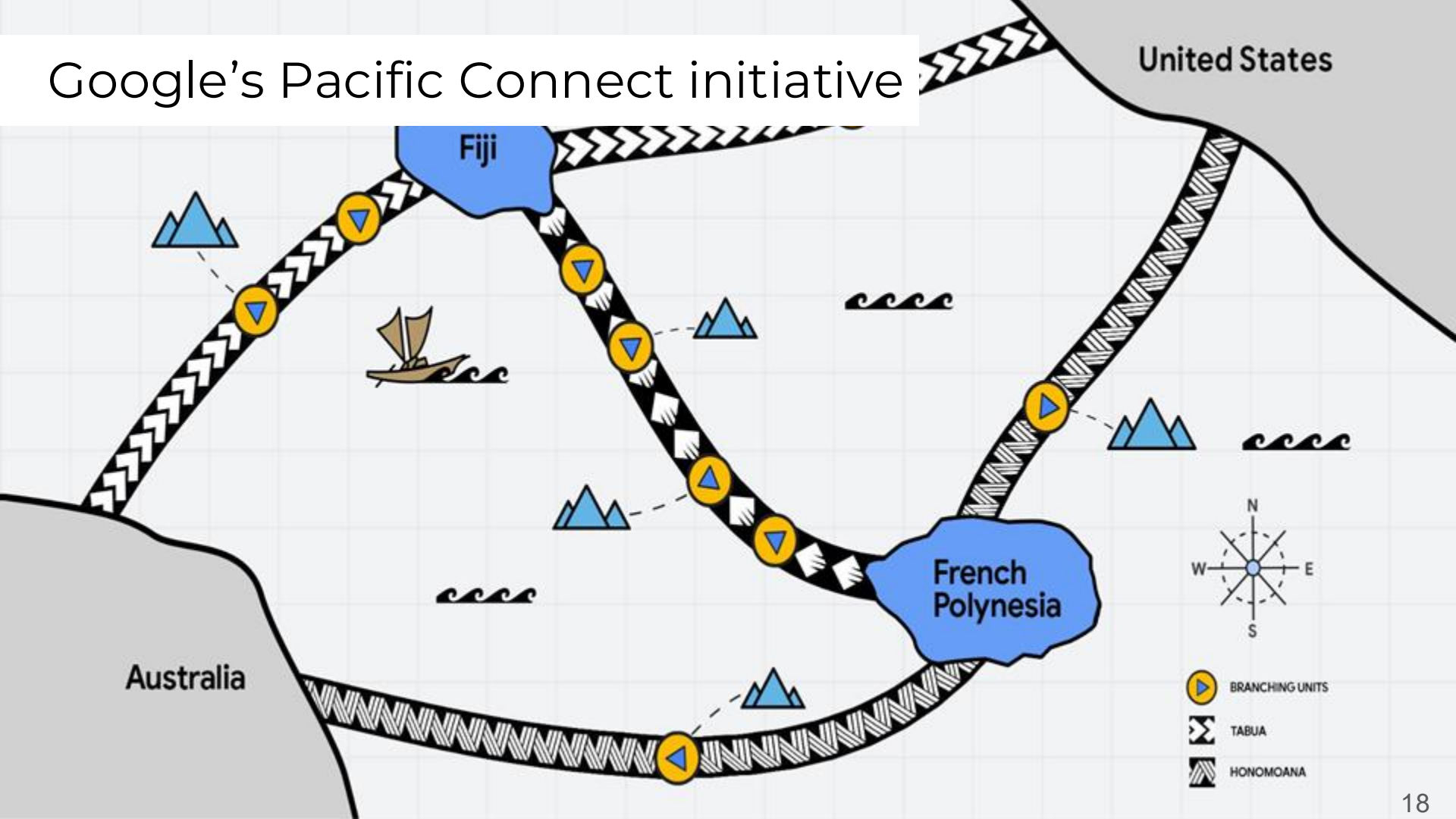
Minilaterals & hyperscaler partnerships

- Coral Sea Cable (Australia ~2018)
- Palau (US, Japan, Australia)
- East Micronesia (US, Japan, Australia)
- Google’s Pacific Connect
  - Tuvalu (Australia, Japan, New Zealand, Taiwan, US) + Google

Google’s web of cables in the Pacific

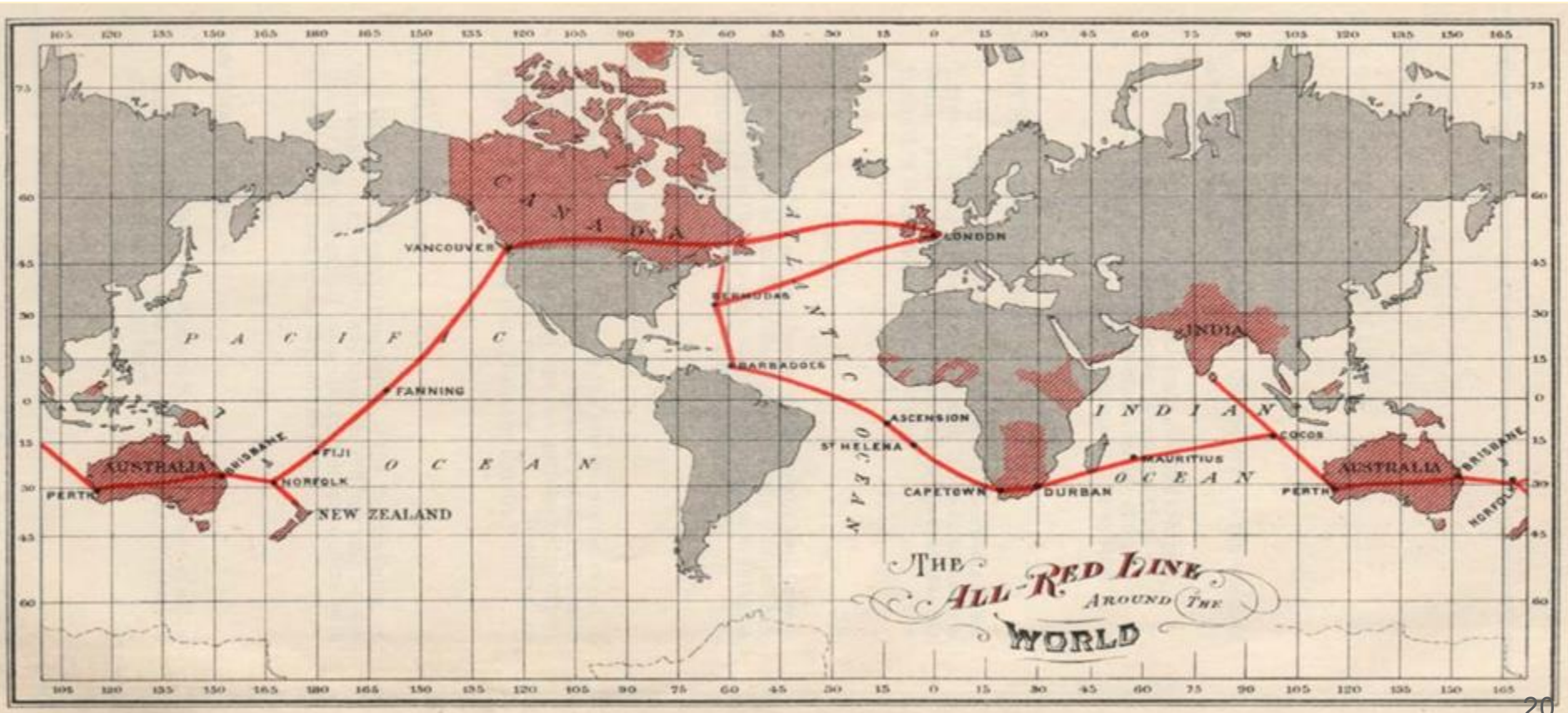


Google’s Pacific Connect initiative



The effect on the security of telecoms networks

Governments see cables as strategic assets



Wartime targets

- **Spanish-American War (1898)** - Within days of the start of the war US Navy cuts undersea telegraph cables to isolate Spain from its colonies.
- **First World War (1914)** - Within hours of declaring war, Britain cut Germany's cables, forcing traffic onto British lines and enabling the world's first global communications surveillance system.

Peace-time surveillance

- **Cold War** (1970s) - Operation Ivy Bells. US cable tapping of Soviet cable
- **Snowden** disclosures (~2014) - interception of transatlantic cables

Now

- This isn’t only about sabotage in war or covert espionage.
- Openly and actively shaping global networks through local legal and regulatory levers; international partnerships and alliances
- Era of hybrid warfare
  - Eg. Cable cutting & other irregular activity in Baltic Sea and Taiwan
  - Cyber attacks

Cyber attacks

- Salt Typhoon access into US telecoms operators
- Attempted cyber attack on systems managing submarine cables out of Oahu, Hawaii.
- Manipulating networks, changing data flows and data collection
- Disrupting normal data transmission over subcables

Opportunities for Australia

Winners and Losers

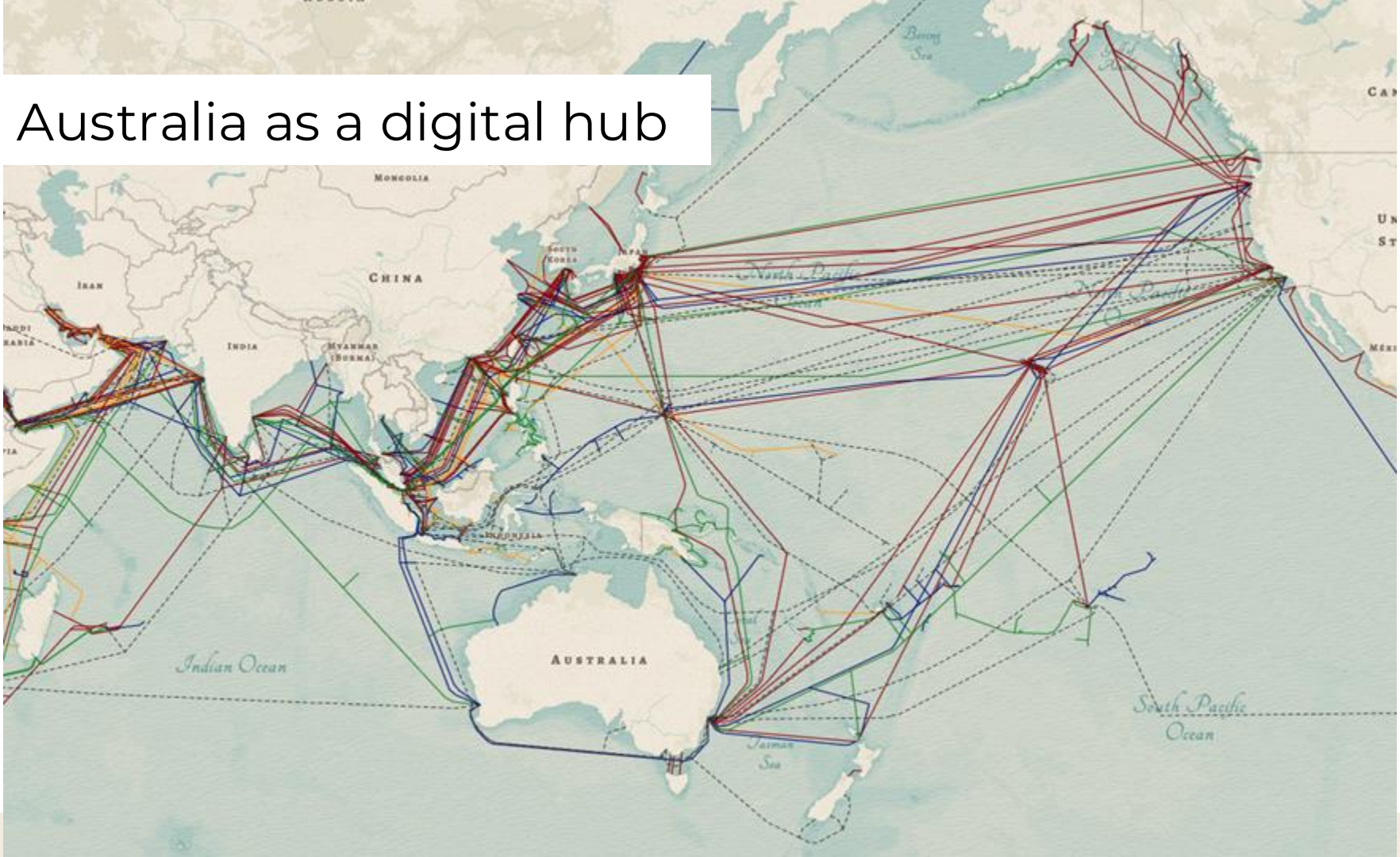
👎😭 **Losers**:

- Hong Kong loses its appeal as a regional cable hub
- Pacific island countries in geopolitically tricky position

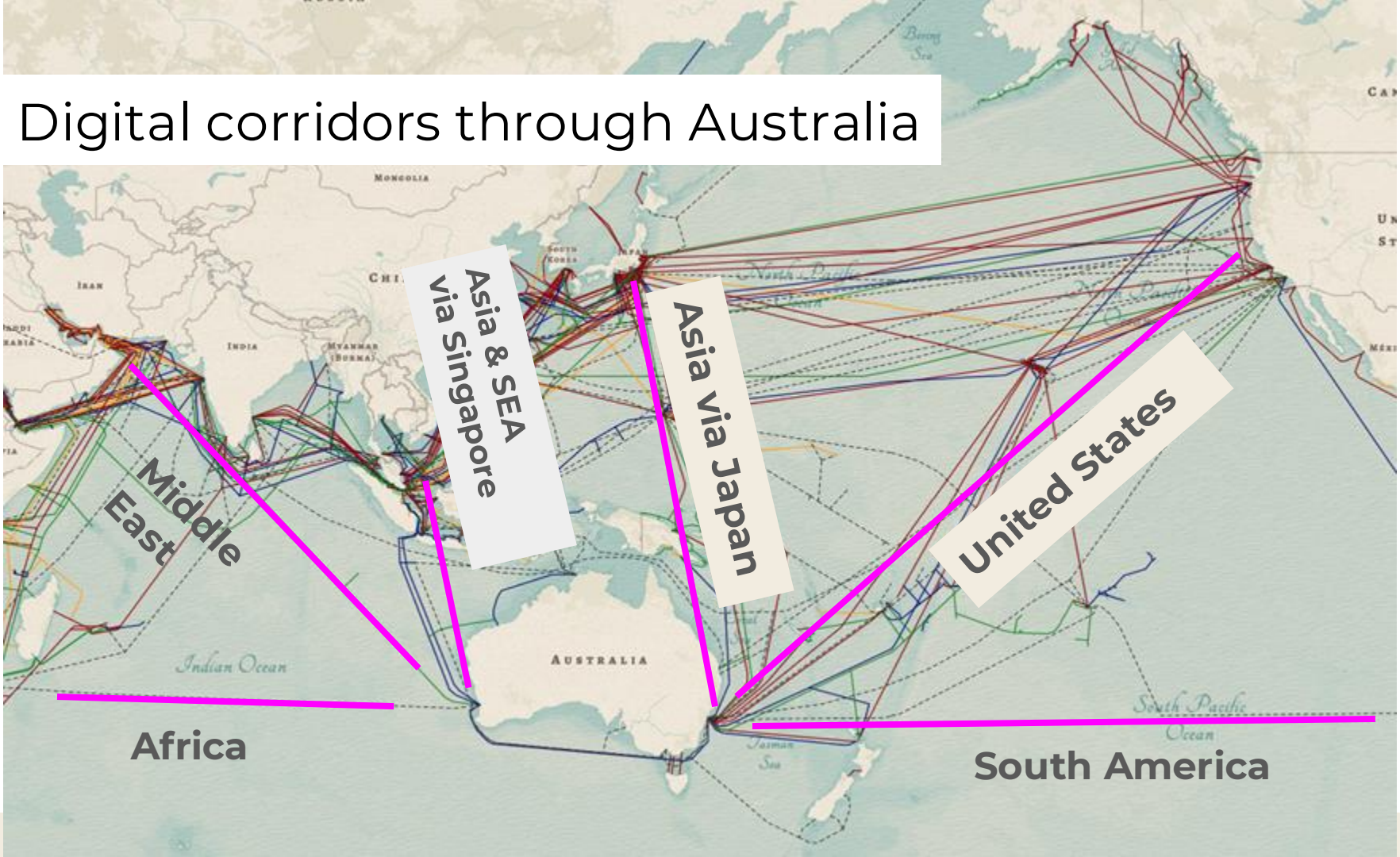
🏆🙌 **Winners**:

- Southeast Asia receives more direct cables
- Australia rises as a digital hub and more reliable, safer, alternative route for the Indo-Pacific region

Australia as a digital hub



Digital corridors through Australia



Summary

- The subsea cable industry is no longer dominated by telcos; it is now shaped by two key factors: **geopolitics and hyperscalers.**
- Cables are **strategic assets** that enable the modern digital economy and carry more than just data—they represent **sovereignty and power**.
- Governments are increasingly concerned with **national security and resilience** and are using legal and political levers to influence cable routes and supply chains to ensure self-sufficiency and security.
- These geopolitical tensions are causing cable routes to be rerouted away from the most direct paths. This is **positioning Australia** a more reliable and safer alternative route for the Indo-Pacific, positioning it **as a digital hub**.

Takeaways

- Submarine cables are not just about connectivity
  - Geopolitical tensions pose threats to network security.
  - Countries are competing for control (and security) of the infrastructure and access to the data.
- Opportunities for Australia
  - Digital connectivity hub and more reliable alternative route for the region
  - Sustainable data centres

go.subcables.au → https://www.aspi.org.au/report/connecting-indo-pacific-future-subsea-cables-and-opportunities-australia