

AI發展與社會影響

簡立峰



AI時代：台股市值世界第六

The Global AI Race is Supercharging Taiwan's Economy: 2025 GDP Growth Rate: **8.68%**

1	 United States	73,300,000
2	 China	17,100,000
3	 Japan	8,190,000
4	 Hong Kong	7,410,000
5	 India	4,970,000
6	 Taiwan	4,470,000
7	 Canada	4,440,000
8	 South Korea	4,040,000
9	 United Kingdom	3,990,000
10	 France	3,450,000



Source: <https://www.macromicro.me/series/687/tw-market-cap>

AI Keeps Getting Smarter!

2024: 語言理解、閱讀、問答、數學 → 2025/2026: 推理、規劃、代理 ...

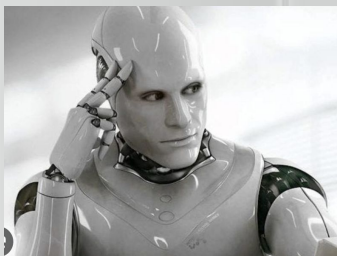
2024: Gemini達到奧林匹亞數學銀牌

2025: Gemini/GPT5 達到奧林匹亞數學金牌

2025: Gemini/GPT5達到 世界程式大賽金牌 (ICPC)

2025: Gemini 3 宣稱: 每項能力都是博士級、讓你實現夢想

5年內出現 AI 愛因斯坦、AI 牛頓 (Google 前董事長 Eric Schmidt)



towardsdatascience.com

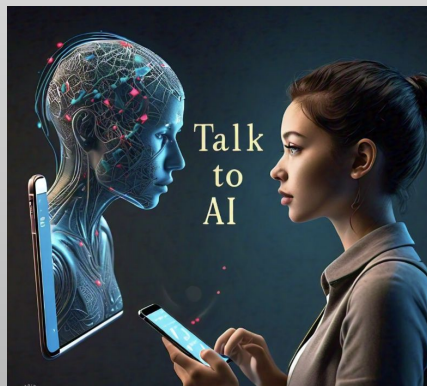
AI進入日常生活

AI Changes the Way We Live

2011

2025

Mobile Everyone & Anywhere



態度兩極: 好玩 or 工具人

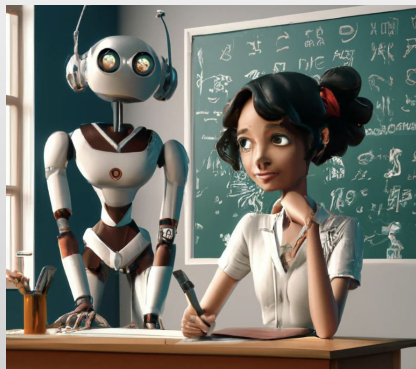
對話: Command to **Conversation**

代勞: Searching to **Asking**

陪伴: Connecting to **Companion**

協作: Tools to **AI Collaboration**

AI 改變工作、學習方式



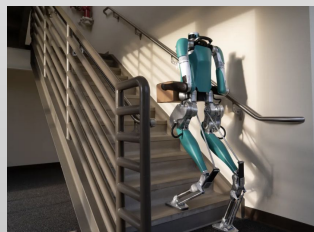
Source: The-Decoder

- AI通過美國醫師、律師、會計師考試
- 台灣指考可以上台大醫科
- ChatGPT 80% 使用量來自學校



Waymo

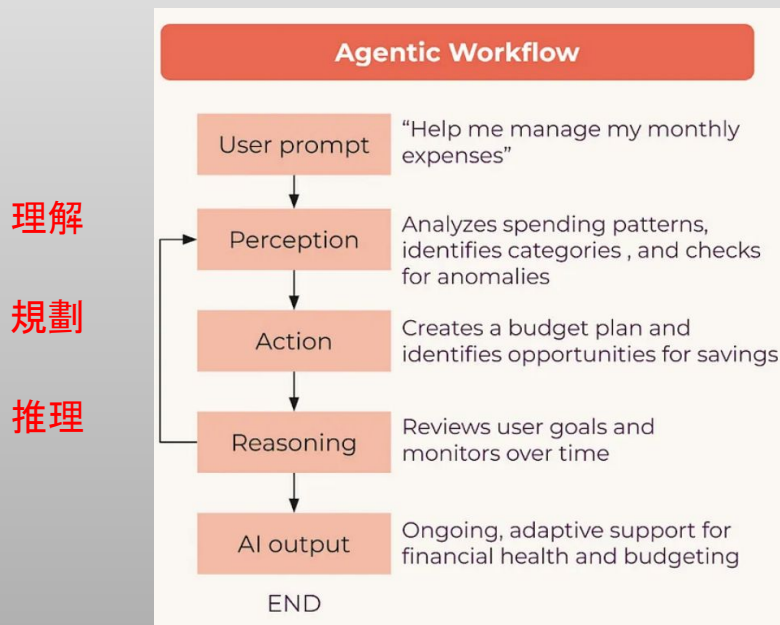
舊金山/LA
WayMo 無人計程車
每週15萬增加到**50 萬人次付費、
11城市、3,000輛車**



Amazon 人型機器人
庫房搬箱 (Q1) 到府卸貨 (Q2)

AI in 2026: Agentic AI

LLMs from Answers to Actions



<https://medium.com/@jinglin.lee/at-your-service-how-ai-agents-are-redefining-the-future-e594ac4bd215>

2026 DeepSeek 事件

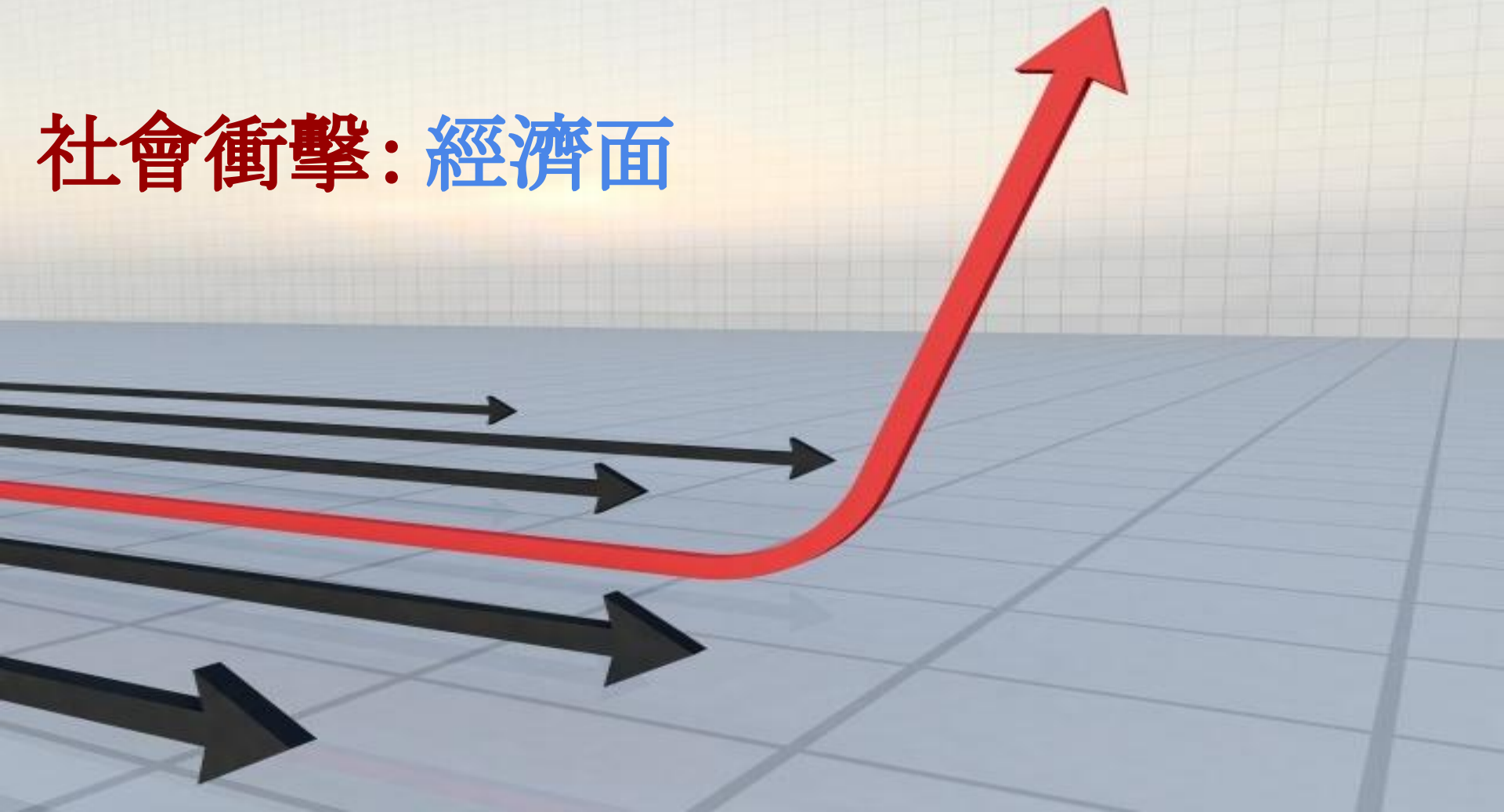
個人代理: OpenClaw(小龍蝦)

- [Edge AI Killer App](#)
- 一人創業興起
- 購物、預約、每日簡報、投資監控 ...

企業代理: Claude Code/ Cowork

- [AI Agents in Enterprise 加速](#)
- 採購、排行程、分析、稽核、預警
- IT、財務、法務、研究 ...
- 企業流程再造, 員工職能調整

社會衝擊：經濟面



經濟面：生產力重組與分配挑戰

人力密集轉向**資本與算力密集**

- **資本最大化**

- 財富向擁有大型模型、算力與數據的資本方集中，擴大貧富差距

- **企業轉型成AI代理型企業 (Agentic Enterprise)**

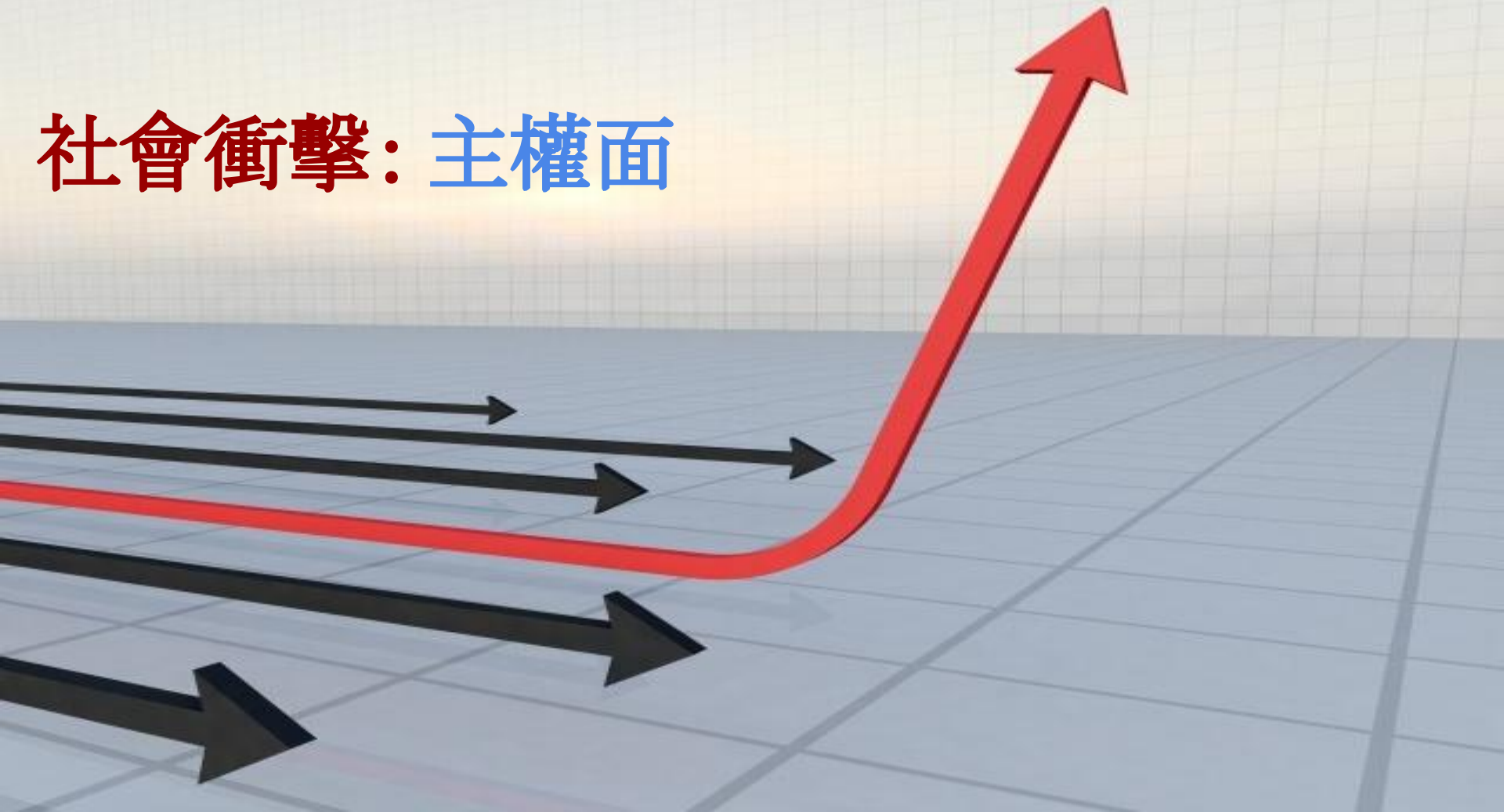
- 企業大量使用「AI Agent」進入工作流程
- 組織扁平化，初階白領 (Entry-level white-collar) 面臨失業

- **薪資極化與超級使用者 (Super-user)：**

- 「一人公司」顛覆中小企業，極小規模卻高 產值
- 能駕馭 AI 的「超級使用者」獲高報酬
- 無法人機協同的人員面臨挑戰



社會衝擊：主權面



欠缺AI自主：威脅國家發展

- **基礎建設**
 - 水電、道路、交通等基建大量依賴 AI智慧管理
 - 雲端AI由外國、外地掌管
- **教育、文化**
 - “Token”經濟背後的強勢霸權
 - 文化教育主導性喪失
- **政府、法治**
 - 政府運作效能、安全高度依賴外國模型、服務
- **國安、國防**
 - 國家安全難以完全自主



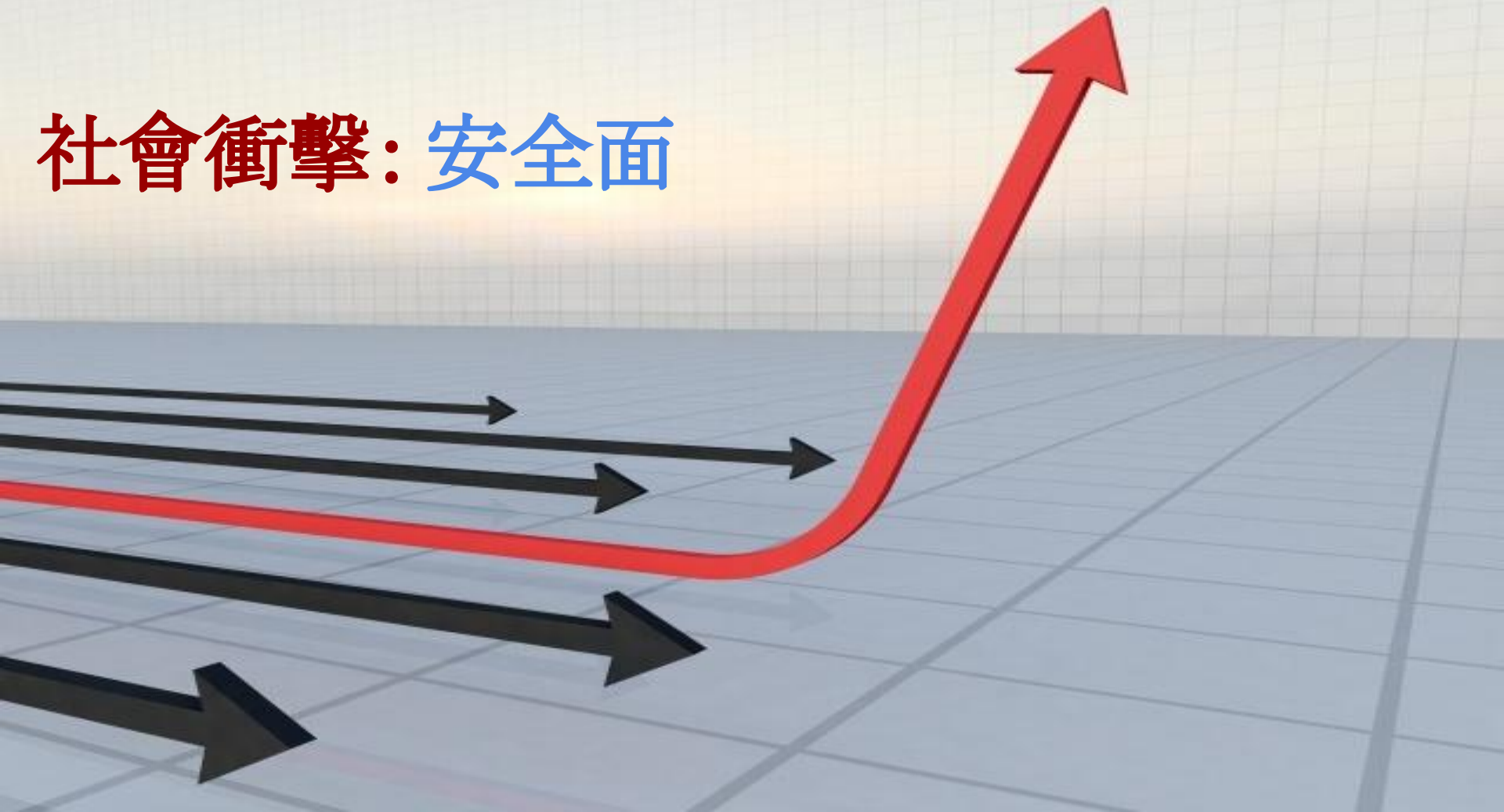
AI時代的主權挑戰

Sovereignty in the Age of AI Dominance

- **主權 AI**
 - 指在國家框架下所創建、部署和治理AI系統，要考慮資料主權、監管合規性和基礎設施控制
 - **Sovereign AI** : refers to the creation, deployment, and governance of AI systems within a nation framework that prioritize data sovereignty, regulatory compliance, and infrastructure control
- **各國主權AI意識**
 - 必須發展符合自身語言、文化與價值觀的模型，以維護資訊主權與數據安全
- **監管與治理兩難**
 - 政府面臨「鼓勵創新」與「防止風險」的拉鋸
 - 過度監管擔心科技落後，放任不管導致社會失序

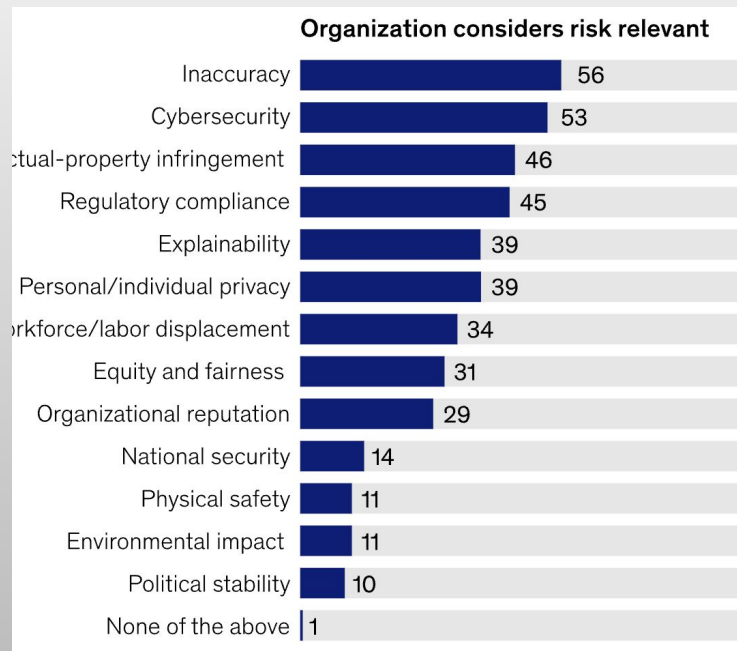


社會衝擊：安全面



AI 造成資安風險

(AI comes at a Cost, not a Free Lunch)



Source: Mckinsey & Company

社會安全：信任體系重建

- **資訊真假難辨 (Information Integrity)**
 - Deepfake (深偽技術) 讓影音、圖像與文字可低成本偽造
 - 「眼見不為憑」, 易引發詐騙、認知作戰與選舉操弄
- **發展兩極化與數位鴻溝**
 - 不同族群對 AI 使用能力差異, 產生「數位原住民」與「數位難民」
- **信任治理**
 - 需要建立新的驗證機制 (如數位浮水印、區塊鏈溯源)
 - 從技術層面轉向「**制度層面**」的信任建設

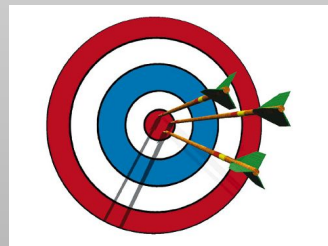


Source: ITNext

公部門：建立法治與標準

政府的角色是「守門員」，負責制定遊戲規則並確保公平性

- **推動數位身分與溯源技術**
 - 如要求 AI 生成內容 (AIGC) 必須包含浮水印，並利用區塊鏈技術建立溯源機制
- **敏捷監管與沙盒計畫**
 - 在特定領域 (如醫療、金融) 先行試點監管，並根據回饋調整法規
- **公共算力與數據平權**
 - 政府應提供公共算力平台 | 高品質的本土語料庫 (如「繁體中文大型語言模型」)、驗證標準與機制，確保公平使用機會



私部門：負責任 AI (Responsible AI)

企業是技術的開發者與應用者，其治理核心在於「透明」與「當責」

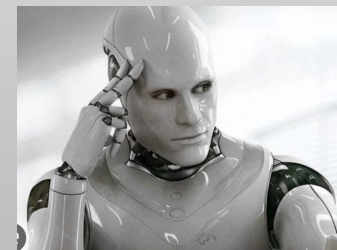
- **演算法透明度與可解釋性 (Explainable AI, XAI)**
 - 企業開發模型或應用，應致力於讓 AI 的決策過程不再是「黑盒子」
 - 尤其在涉及徵才、貸款、保險等關鍵影響時，必須能解釋決策依據
- **建立倫理審查委員會**
 - 企業應設立倫理小組，評估 AI 產品是否帶有族群歧視、性別偏見或侵害隱私
- **Agentic Enterprise 的合規審計**
 - 企業 AI Agent 開始自主運作，須有審計系統紀錄 AI 行為 (Logs)
 - 確保人機協同的過程中有跡可循



個人面：從被動接收到主動驗證

AI 時代個人需要更強大的心理素質與辨識技巧

- **零信任原則 (Zero Trust Mindset)**
 - 預設「所有未經多方驗證的資訊都可能是 AI 生成的」，尤其在涉及金錢、情感與政治判斷時，應採取多管道查證
- **學習提問與驗證的能力**
 - 學習如何與 AI 協作，並具備對 AI 結果進行「二度驗證」的能力
- **數位足跡的自我管理**
 - 意識自我數據價值，保護個人生物特徵，防止被挪用作偽造



教育面：培養 AI 時代的職能與識讀

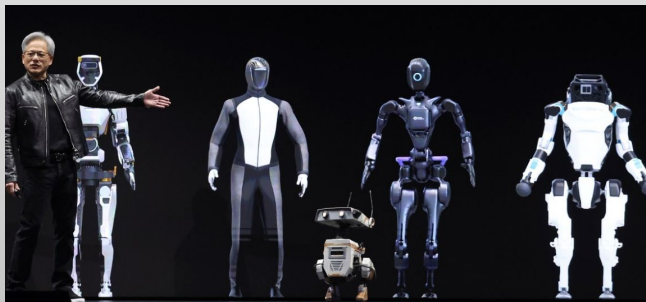
透過教育建立社會整體的「防毒意識」

- **AI 識讀教育 (AI Literacy)**
 - 教導學生識別 Deepfake、假新聞、詐騙的特徵，理解 AI 生成內容的原理與局限
 - 強調「定義問題」而非「尋找答案」，
- **師資轉型**
 - 教師需從純知識傳授者，調整為學習導師，以及「AI 協作教練」
 - 引導學生利用 AI 探索、培養自主學習
- **數位平權**
 - 確保弱勢學生獲得 AI 工具與算力，避免教育階級化



成為 AI 的指揮家！

Becoming the Conductor of AI



Nvidia

繫好安全帶，準備起飛！

Thanks!

