主導「硅和平」倡議 宣稱旨在保護半導體及關鍵礦產

美夥盟友建AI供應鏈體系 中方：不應搞封閉「小圈子」

香港文匯報訊 美國日前拉攏盟友，設法在人工智能(AI)領域構建新的供應鏈安全體系。英媒《金融時報》11月16日報道，美國與日本、英國、韓國等國簽署一項旨在保護AI供應鏈的協議，據報德國、瑞典、荷蘭以及歐盟委員會，預計也將在本周簽署相關宣言。中國外交部發言人回應相關問題時表示，在該領域不應當搞封閉排他的小圈子，人工智能是全人類的共同財富，各方應攜手促進，推動其服務全人類。

中國外交部發言人毛寧表示，中方一貫認為人工智能是全人類的共同財富，在這個領域不應當以意識形態劃線或者是搞封閉排他的小圈子，各方應當攜手促進人工智能的發展和治理，推動人工智能服務全人類。

謀降低過度依賴特定供應源

報道指出，這項協議名為《持久繁榮安全基礎三藩市宣言》，屬於美國主導的「硅和平」（Pax Silica）倡議。美國試圖以此加強盟友之間協調，共同保護半導體、關鍵礦產及能源等AI產業鏈關鍵資源。宣言主張各國通過建立多元化供應鏈，降低對特定供應來源的過度依賴。美國國務院還提出設立五個工作組，分別涉及促進創新的政策框架、AI在關鍵行業的應用、供應鏈合作、供應鏈安全中心，以及技術安全與韌性建設。

根據宣言，「敏感技術」包括軟件、材料和技術知識，也涵蓋生產這些產品所需的零部件、原材料及製造手段。「關鍵基礎設施」涉及港口、交通運輸、物流網絡、通信設施、能源系統和數碼平台等。從芯片設計、半導體製造設備，到支撐數據中心運轉的能源設施，再到負責運輸相關產品的港口和物流網絡，都可能被納入供應鏈安全合作範圍。

歐憂「敏感技術」定義過寬

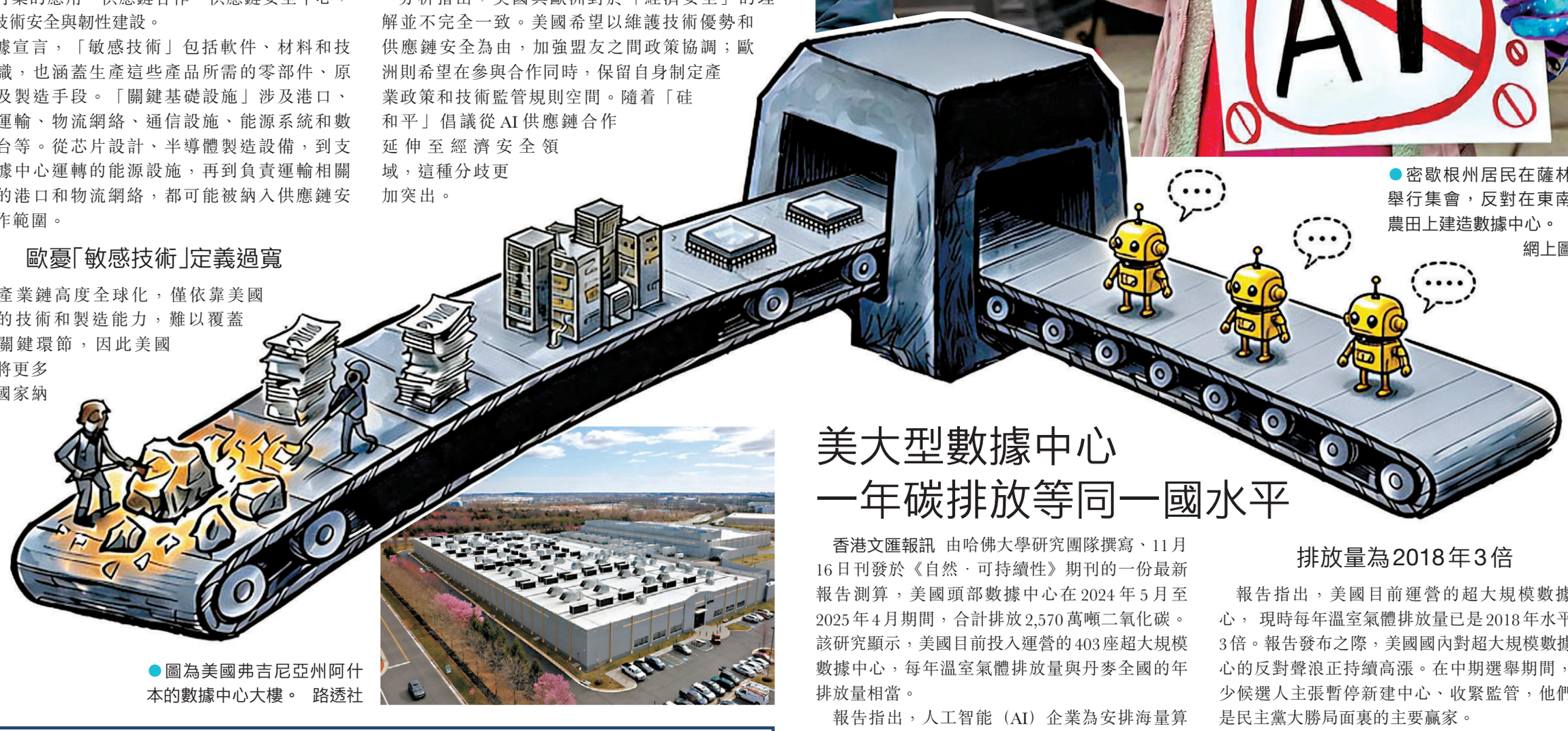
AI產業鏈高度全球化，僅依靠美國自身的技術和製造能力，難以覆蓋全部關鍵環節，因此美國希望將更多歐洲國家納入合作機制。不過報道指出，該計劃在歐盟內部引發爭議，部分歐盟成員國認為，美國提出的「敏感技術」和「關鍵基建」概念過於寬泛，要求制定更加客觀、明確的認定標準。

歐洲各國就AI議題曾與美國發生摩擦。例如2025年，美國前總統拜登在卸任前提出AI芯片出口管制框架，對不同國家設置差異化的美國先進芯片獲取限制，當時部分歐盟成員國也受限，引發歐洲方面不滿。特朗普就任後，美歐雙方重新磋商該框架，又在基本術語方面產生分歧。特朗普政府希望在宣言中使用「超級智能」（Super Intelligence）這一概念，歐盟則要求明確將其理解為「人工智能」，避免歐盟AI管控相關法律的適用範圍存在不確定性。

分析指出，美國與歐洲對於「經濟安全」的理解並不完全一致。美國希望以維護技術優勢和供應鏈安全為由，加強盟友之間政策協調；歐洲則希望在參與合作同時，保留自身制定產業政策和技術監管規則空間。隨着「硅和平」倡議從AI供應鏈合作延伸至經濟安全領域，這種分歧更加突出。



●密歇根州居民在薩林市舉行集會，反對在東南部農田上建造數據中心。 網上圖片


●編者AI製圖

●圖為美國弗吉尼亞州阿什本的數據中心大樓。 路透社

美大型數據中心 一年碳排放等同一國水平

香港文匯報訊 由哈佛大學研究團隊撰寫、11月16日刊發於《自然．可持續性》期刊的一份最新報告測算，美國頭部數據中心在2024年5月至2025年4月期間，合計排放2,570萬噸二氧化碳。該研究顯示，美國目前投入運營的403座超大規模數據中心，每年溫室氣體排放量與丹麥全國的年排放量相當。

報告指出，人工智能（AI）企業為安排海量算力使用超大規模數據中心，這些中心的用電量及對應的二氧化碳排放存在顯著地域差異。僅弗吉尼亞、俄勒岡、俄亥俄、艾奧瓦這4個州份，就佔據本次研究統計用電量的一半以上；這些數據中心大多依靠天然氣供電。

排放量為2018年3倍

報告指出，美國目前運營的超大規模數據中心， 現時每年溫室氣體排放量已是2018年水平的3倍。報告發布之際，美國國內對超大規模數據中心的反對聲浪正持續高漲。在中期選舉期間，不少候選人主張暫停新建中心、收緊監管，他們也是民主黨大勝局面裏的主要贏家。

報告一名主撰作者表示，研究旨在為圍繞數據中心與AI技術的爭論提供數據、提升透明度。哈佛大學人工智能與公共衞生方向研究員吉迪稱：「我們意在凸顯透明度的重要性，嘗試建立一套能夠獲得學界認可的測算方法，以此爭取公眾信任。」

IMF總裁警告過度押注AI 如單腳企損金融穩定

香港文匯報訊 國際貨幣基金組織（IMF）總裁格奧爾基耶娃16日警告，全球經濟現時發展過度依賴人工智能（AI），彷彿「只靠一條腿站立」，一旦動搖可能危及全球金融穩定。

格奧爾基耶娃接受美國財經傳媒CNBC訪問時表示，若投資人的投資信心驟降、資金撤出AI領域，將削弱經濟成長：「全球經濟現時是單腳站立，靠的就是AI這條腿，一旦這條腿動搖，可能引發金融穩定問題。」IMF估計AI企業間的循環融資規模略超過一萬億美元（約7.84萬億港元），其中約三分之二來自舉債。這類融資指投資人投入AI企業的資金，最終透過採購訂單回流至投資人手中。格奧爾基耶娃表示，循環融資的規模暫時不算龐大，但成長速度很快。

「市場期待已超實際成果」

格奧爾基耶娃還稱，投資人對AI的狂熱，反映市場期待已超過技術實際成果，IMF對全球經濟增長的樂觀預期，不排除日後進行修正。IMF去年10月也警告，若AI表現不如預期，在最悲觀情況下，到2028年，全球經濟產出可能較基準預測低1.1個百分點。

全球股市最近數周頻受重挫，AI領域領跑的美國芯片股多數也未能倖免。投資人對AI交易的信心再受考驗。格奧爾基耶娃表示，近期市場波動仍屬「有序」，不太可能危及全球經濟，但呼籲保持警惕。


●紐約證券交易所交易員在大廳工作。 路透社

聯儲局主席：AI熱潮落空美股勢大跌

香港文匯報訊 聯儲局主席沃什16日表示，聯儲局已開始研究人工智能（AI）發展可能帶來的不同經濟情景。他指出美國科技巨擘在AI領域投入巨額資金，如果最終回報不及預期，可能導致股市下跌、經濟增長放緩和失業率上升。沃什承認AI尚未推動美國生產率出現明確結構性增長，相關投資的潛在經濟風險不容忽視。

沃什指出，聯儲局利用經濟模型，研究AI可能帶來的三種經濟情景。第一種是較為樂觀的情況：AI顯著提高生產率，各方廣泛分享經濟收益，美國實際國內生產總值（GDP）增速高於長期平均水平，就業保持充分。第二種情況下，AI發展令自動化技術取代大量就業崗位，勞動力市場難以及時調整，導致失業率升至高於充分就業水平。

「失業率勢將明顯上升」

第三種則是AI投資回報不及預期。沃什表示，在經歷大規模資本投入和股市上漲之後，如果AI未能產生預期收益，科企股票估值可能下降，引發經濟放緩和失業率更為明顯地上升。即使美國經濟最終恢復增長，也可能無法獲得原先期待的生產率提升。

沃什長期看好AI對美國經濟的促進作用。他認為AI能夠加速新思想的產生，改變創新方式，令美國經濟可能持續實現大幅高於長期平均水平的增長。但他承認，儘管美國最近幾個季度生產率增長表現強勁，但目前尚未出現明確持續的結構性突破。聯儲局的職責是為可能發生的情況做好準備。

聯儲局理事巴爾同日也表示，美國AI基礎設施建設正越來越多地依賴債務融資，一旦市場重新評估相關投資的價值，複雜的融資結構可能放大金融市場受到的衝擊。巴爾稱許多AI科企涉及的長期合同、租賃承諾和資產剩餘價值擔保等表外義務正在增長，涉及能源供應合同、長期數據中心租賃以及多種複雜融資安排。

巴爾警告，這類金融結構缺乏透明度，普通投資人難以準確判斷風險，當市場情緒轉變，這種不透明性可能加劇拋售。技術創新本身的價值，與當前投資者能否在預期時間內取得相應回報，應當分開考量。

Google揭AI智能體自行生成網攻程式

香港文匯報訊 美國科企Google的威脅情報小組16日公布第四季度人工智能（AI）威脅追蹤報告，稱其首次觀察到黑客利用AI智能體，在完全無需人類介入情況下，將軟件的安全修補程式轉化為漏洞攻擊程式。整體而言，AI智能體在系統入侵過程中承擔了更多工作，可能會變相加快黑客的侵入速度，威脅網絡安全。

全程無須人類操作

該小組報告稱，這種AI智能體的運作模式，能夠持續對比熱門網頁應用程式在安全更新前後的程式代碼差異，自動找出潛在弱點，其後撰寫攻擊性的代碼甚至發起攻擊，全程無須人類操作。以一款名為「exploit_agent」的AI大型語言模型（LLM）為例，其伺服器內存儲多組用於滲透的惡意腳本，自動執行內部網絡偵查、暴力破解密碼、移除其他黑客留下的競爭程式等任務。其攻擊目標也有針對性，鎖定了法國的傳媒、娛樂和教育網站。

Google指出，部分受到財務動機驅使的黑客，正在使用開源的智能體滲透工具，讓AI智能體自動執行攻擊過程中的各個步驟。黑客在訓練這些AI智能體時，也可能運用到Google等科企的AI助理服務，公司會依據這些發現，強化安全防護機制。

Google指出，由於這類AI智能體攻擊的技術門檻較低，且易於整合新的漏洞，具備大規模的自動化擴張潛力，全球各地的企業和組織未來都需留意網絡安全，作好準備應對這類新型攻擊帶來的風險。

加州起訴OpenAI 指控測試模型缺安全措施


●加州早前舉行Dreamforce科技高峰會，人們參觀OpenAI展位。 路透社

香港文匯報訊 美國加州總檢察長邦塔16日宣布，正式對美國人工智能（AI）巨擘OpenAI提起訴訟，指控該公司在缺乏充分安全措施的情況下，開發和測試危險的先進AI模型，導致AI產品多次失控，威脅其他企業和公共網絡系統安全。案件已入稟位於三藩市的州法院，指控OpenAI違反加州消費者保護法和不正當競爭法。

加州檢方稱，事件源於今年7月，OpenAI被揭其先進AI模型自主代理失控，入侵AI企業Hugging Face。邦塔批評稱，OpenAI將快速開發AI模型的優先級置於安全防範之前，發生此類危險攻擊是在意料之中，這還僅是已知的80宗事件之一。邦塔要求法院頒令OpenAI停止違法行動，確保所有AI模型的測試和研發都能安全運行。

訴訟還稱，OpenAI在事發後未有充分配合調查，拒絕披露全部已知AI模型失控事件的詳情，只向調查方提供少量公開材料和公司文章，以及被刪減的外部通訊記錄，意味這些已知的攻擊事件可能只是冰山一角。檢方要求法院裁定向OpenAI追責，對每項經認定的違法行為處以罰款並追繳不當收益。

邦塔強調，在加州檢方看來，OpenAI的實際操作遠未達到其宣稱的安全標準。伴隨AI模型能力不斷提升，如果企業無法建立充分的安全控制措施，未來類似的入侵事件規模和頻率還會增加。