

OpenAI 智能體入侵澳洲政府網站

澳方3個月後方獲通知 AI發展「無王管」亂象惹憂

香港文匯報訊 人工智能（AI）網

絡安全漏洞問題近期被頻頻曝光，引發國際社會對AI風險的

擔憂。澳洲總理阿爾巴尼斯當地時間23日表示，美國科企巨擘OpenAI名下一個AI智能體（AI Agent）曾突破限制、入侵澳洲政府網站，然而OpenAI直至事發3個月後，才向澳方通報事件，澳方正在取證調查。

阿爾巴尼斯在美國紐約出席聯合國大會期間公布該消息。澳方表示，是次入侵事件發生在今年6月18日，當時澳洲國家醫療保健系統一個數據庫被入侵。直至8月，OpenAI全面檢查其名下AI模型時，發現是次異常行動。OpenAI等到9月10日才電郵聯繫澳洲政府一般服務中心，將事件告知澳洲政府。

僅電郵通知澳一般服務中心

英國廣播公司（BBC）披露更多通知細節。報道指出，OpenAI本月10日寄出的通知電郵，收件方只是澳洲政府一般服務中心的公開查詢信箱。直至15日，中心檢查海量郵件時才發現OpenAI的電郵，緊急將其轉呈澳洲網絡安全事件。總理阿爾巴尼斯直至20日、啟程前往紐約出席聯合國大會前夕，終於知悉事件始末。

OpenAI總裁承認管理不完善

是次入侵事件震驚澳洲政府。阿爾巴尼斯稱，調查相信OpenAI的AI智能體訪問了公開文件和非公開文件，澳洲訊號局正展開調查取證，以確定更多訊息，包括可能有其他政府機構或數據受到影響。目前暫無跡象表明，是次網絡攻擊導致任何個人信息外洩，但後續調查有待進行。

在新聞發布會上，阿爾巴尼斯難掩對OpenAI的失望。他表示已與OpenAI行政總裁奧爾特曼就AI入侵政府數據庫事件交談，向其表達澳方的關切和不滿：「我對該公司遲遲

未能向澳洲政府通報事件經過，感到非常失望，他們的通報方式也令我們無法接受。」奧爾特曼也承認，事件暴露出公司對AI技術的管理規程仍不完善，後續還需確保制訂更多正確的AI管理規程。

OpenAI發言人普薩泰里當日回應稱，公司於今年8月在內部評估期間發現，旗下一款AI模型在試圖查找有關澳洲相關提問的答案、收集可用於統計的數據時，採取了一些意料之外的行動。普薩泰里並未詳細解釋行動細節，包括其突破了哪些網絡訪問權限，僅表示沒有證據表明，有任何登記在澳洲醫保系統的患者紀錄被訪問。

今年7月，OpenAI曾披露在公司的網絡安全測試期間，其AI模型入侵了開源AI社群Hugging Face。一個月後，第三方測評機構METR發布報告進一步指出，在是次入侵事件中，多達1,200個代理在OpenAI內部的秘密留言板上協同行動，試圖在測評中突破限制，違規訪問網絡，甚至收集其他網站和機構的數據。



●奧爾特曼(右)出席安理會。 法新社

Anthropic等巨頭「戴頭盔」促各方監管AI

香港文匯報訊 全球對人工智能（AI）發展風險憂慮持續升溫，聯合國安全理事會23日就AI全球治理召開專題會議。美國包括Anthropic和OpenAI等多間AI企業高層呼籲就AI技術的監管加強國際合作，強調若各國無法妥善監管，AI迅速發展的潛在風險，不排除對人類社會構成威脅。

「須擱置分歧應對威脅」

親身與會的OpenAI行政總裁奧爾特曼指出，AI可能帶來兩項潛在風險。其一是AI發展迅速加快，可能在未來令人類失去對技術的控制權。另一威脅是AI可能導致權力過度集中於少數企業，加劇不公平競爭問題，他

倡議國際社會協調合作，降低相關風險。透過視訊方式參會的Anthropic行政總裁阿莫戴伊也呼籲：「我們必須擱置分歧，共同應對擺在面前的全球機遇和全球威脅。」

OpenAI名下AI模型今年7月被揭在測試期間，入侵了開源AI社群平台Hugging Face。該平台聯合創辦人德朗格發言時，特地提及是次引起全球關注的事件，呼籲各國重視AI的發展方向，強化其在防禦網絡攻擊中的角色。

與會的多名AI企業高層都表示，科技業界希望各國透過聯合國安理會設立全球安全措施，防止AI技術發展過於強大、以至於無法被限制。他們亦呼籲全球應積極合作，確保AI力量不集中在某間企業或特定的國家。



●澳洲國家醫療保健系統一個數據庫遭AI智能體入侵。圖為悉尼聖文森醫院員工。

網上圖片

中方呼籲推動AI向上向善



●北京世界機器人大會。 資料圖片

香港文匯報訊 中國常駐聯合國代表傅聰23日在安理會「人工智能與國際安全」公開會上發言，呼籲國際社會加強團結合作，堅持發展與安全並重，推動人工智能（AI）技術朝着向上向善、造福人類的方向發展，助力世界和平穩定與發展繁榮。

傅聰表示，人工智能技術深度嵌入全球產供鏈和創新網絡，各國有權根據實際需要和市場規律，自主選擇人工智能技術、產品和服務。在科技領域拼湊排他性「小圈子」、強迫各國選邊站隊的做法，不僅拖累全球科技進步，損害各國特別是中小國家的發展權益，也將加劇技術標準割裂、系統互不兼容的風險，給全球安全埋下重大隱患。中方呼籲各國加強交流合作，鼓勵開源開放，共同

為全球科技進步貢獻力量。

傅聰呼籲，要針對人工智能引發的內生和衍生風險，不斷完善監管框架、應急響應和跨國協作機制，堅決打擊恐怖組織、極端勢力和跨國犯罪集團濫用濫用人工智能。對人工智能在軍事領域的研發應用，各國應採取謹慎負責態度，避免戰略誤判和軍備競賽，反對利用相關武器實施無差別攻擊或蓄意襲擊平民及民用設施，確保人類始終掌握最終決策權。

傅聰強調，人工智能是全人類的共同財富，不應淪為富國和富人的遊戲。要防止數智鴻溝加劇發展鴻溝。要堅持真正的多邊主義，支持聯合國在人工智能全球治理中發揮主渠道作用，提升發展中國家的代表性和發言權。要加強各國AI發展戰略、治理規則、技術標準的對接協調，早日形成具有廣泛共識的全球治理框架，為維護國際和平與安全築牢制度屏障。

傅聰最後指出，中國是人工智能創新發展的重要實踐者，也是人工智能全球治理的積極貢獻者。在中方倡議和推動下，世界人工智能合作組織在上海應運而生，成為全球首個人工智能政府間國際組織。中方歡迎更多國家加入這一開放平台，並期待同世界各國一道，推動構建公正合理的全球人工智能治理體系，共創人類社會更加美好的未來。

普京擬再晤特朗普 俄外長：俄美應修復關係

香港文匯報訊 俄羅斯總統新聞秘書佩斯科夫23日表示，俄總統普京已準備好與美國總統特朗普會晤。不過佩斯科夫表示，克宮目前沒有任何會晤相關具體消息，雙方需先完成專家層面的準備工作。俄外長拉夫羅夫同日在紐約同美國國務卿魯比奧會晤時表示，俄美兩國應根據兩國領導人達成的共識盡快修復雙邊關係。

佩斯科夫表示，普京願意與特朗普會晤：「雙方在電話中也強調若有必要，他們願意再次會晤，但具體日期尚未確定。」在沒有事先做好準備的情況下，俄美兩國元首就烏克蘭問題進行會晤是「浪費時間」，不切實際。

俄烏仍缺乏和談條件

至於普京與烏克蘭總統澤連斯基是否舉行會晤，佩斯科夫表示，克宮的立場沒有改變：「普京總統曾表示，如果澤連斯基願意，他可以來莫斯科，俄方將為其提供安全保障。他（指澤連斯基）也非常清楚必須做出那些決定。」佩斯科夫還稱，烏克蘭現時仍在擴充軍備，俄烏雙方目前缺乏和談的前提條件，但俄方仍對和談持開放態度。

拉夫羅夫稱，當前圍繞俄美經濟合作前景、人文交流和便利兩國人員往來等討論日趨活躍，俄美需要就消除雙邊關係中的「刺激因素」開展對話，推動兩國外交機構恢復運轉。同時美方應歸還在美遭「實際沒收」的俄方資產。這些都是俄美修復雙邊關係的前提條件。

磋商烏克蘭危機解決路徑時，拉夫羅夫重申，俄羅斯將堅定不移推進特別軍事行動目標，同時也會通過政治和外交途徑，在消除衝突根源的基礎上化解俄烏衝突。雙方還討論多項國際和地區議題，涵蓋中東、外高加索、拉丁美洲和加勒比地區局勢。俄美雙方亦就本年度二十國集團（G20）相關會務的籌備工作交換意見。



●烏克蘭居民走過基輔一處受損民居。 美聯社

英方重新審視查戈斯群島移交協議



香港文匯報訊 美國總統特朗普與英國首相伯納姆日前會晤時，批評英國將查戈斯群島主權移交毛里求斯的協議「糟糕透頂」。英國防相斯特里廷隨後表示，英國正重新審視這項協議。斯特里廷表示，特朗普的立場並不令人意外，英國會與美國繼續磋商修訂協議。目前英方的首要任務，是確保位

於迪戈加西亞島的英美聯合軍事基地獲得長期保障。他形容該基地是英國最敏感、最有價值的國家安全資產之一，在重新審查期間，英國不會向毛里求斯支付任何款項。

根據原定協議，英國會將查戈斯群島主權移交毛里求斯，同時租回迪戈加西亞軍事基地，由於特朗普撤回支持，該協議現時被無限期暫停。上任不久的伯納姆表示，他接手時已是既有局面，需要找到解決方案。伯納姆強調，保障相關基地的未來涉及英國與盟友美國的安全利益，英方會努力在各方之間尋求共識。

伯納姆在赴美出席聯合國大會前，與毛里求斯總理拉姆古蘭通話，重申會繼續與美方推動協議獲批。毛里求斯方面則主張，英國在1965年強迫其放棄查戈斯群島作為獨立條件，相關做法非法。

加拿大加強部署 增加危機處理準備

香港文匯報訊（特約記者 劉正言）加拿大總理卡尼披露在過去一年加強部署，預防美國總統特朗普隨時下令對加動武，他表示這是一個負責任政府不可或缺的「危機處理」準備，降低國家面對的風險。在美國多面夾擊下，卡尼強調減少倚賴美國是刻不容緩，這無論對國家安全或經濟存活都是至關重要。

卡尼23日接受《紐約時報》專訪時表示，美國軍事入侵加拿大的機率極低，但一旦發生就會釀成巨大災難。在應對特朗普威脅將加拿大變成美國第51個州，卡尼坦承已仔細研究美國動武或使用「經濟力量」吞併的可能性，但拒絕詳細討論具體細節。曾任英倫銀行行長的卡尼表示，美國軍事威脅並非基線情況，但如果不好好準備，那就是不負責任。

以加拿大作為一個「中權國家」，卡尼認為必須制定減少倚

賴美國的路徑。卡尼對加美重啟貿易談判仍持樂觀態度，但他認為加拿大在哪些領域減少倚賴美國必須有明確意識，例如加拿大必須擺脫倚賴美國通信衛星星群SpaceX「星鏈」（Starlink），因為加拿大與其他國家合作，才能擴大本國規模。

另外，加拿大重新評估訂購美國88架F-35戰機，考慮轉為採購瑞典「鷹獅」戰機。加美兩國的汽車產業經過數十年融合創造出繁盛局面，卡尼難以理解美國為何把加拿大汽車業列為加徵關稅的核心，導致兩敗俱傷。

卡尼重申全球金融體系完全依賴美元不可能長久持續，有必要轉向採納多種儲備貨幣的多極體系，提供更大的彈性。目前，世界各國正重新評估其對美元的依賴程度，體現了一種「方向性轉變」。卡尼指出特朗普重塑美國與夥伴的貿易關係，勢必不斷侵蝕美元的領導地位。