

OpenAI 代理侵澳醫保數據庫

事發3個月才通報事件 澳總理表不滿

人工智能(AI)網絡安全漏洞問題近期頻頻被曝光，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，美國科技巨擘OpenAI名下一個AI代理(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。

奧爾特曼認管理規程不完善

英國廣播公司(BBC)披露更多通知細節。報道指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。

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代理訪問了公開文件和非公開文件，澳洲信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訊息外洩，但後續調查有待進行。

在新聞發布會上，阿爾巴尼斯難掩對



■阿爾巴尼斯手持國民保健卡，交待遭OpenAI入侵情況。

美聯社

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接觸，向其表達澳方的關切和不滿。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。

美科企聯國籲國際合作監管AI

另外，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。

親身與會的奧爾特曼指出，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。」

與此同時，中國常駐聯合國代表傅聰發言時，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。

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、以致無法被限制。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。

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。

特朗普施壓

英暫停交還查島

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。

稱要保障英美安全利益

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。



■查戈斯群島民眾曾舉行示威，反對將該島歸還給毛里求斯。

網上圖片

普京擬再晤特朗普 俄外長稱兩國應修復關係

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。

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。」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。至於普京與烏克蘭總統會否舉行會晤，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。」

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。拉夫羅夫稱，俄美需要就消除雙邊關係中的「刺激因素」開展坦誠對話，推動兩國外交機構恢復正常運轉。

「分金不勻」為何變「盜竊」?

黃江天 資深法律人



生活與法

上周說到，香港某部門十多位同事合資投注六合彩，中半注彩金達三千多萬元。負責投注者要求獨佔其中一千萬元，餘下再平分，商議不果就請假失聯，警方以涉嫌「盜竊」將其拘捕。

一件「分金不勻」的民事糾紛，為什麼演變成涉嫌「盜竊」？根據《盜竊罪條例》第9條，盜竊是刑事罪行，定罪可處監禁10年。第2條規定：任何人若無合法授權或合理辯解，而不誠實地挪用屬於他人的財產，意圖永久剝奪其財產所有權，即屬「盜竊」。要構成盜竊罪，必須符合四大要素，包括：1) 財物屬於他人；2) 行為人並無合法授權而挪用

財物；3) 存有「不誠實」意圖；及4) 意圖永久剝奪他人對財物的權利。

所謂挪用，指行為人做出只有物品所有人才能做的事，把他人財產當自己財產來用；他人的財產，指該物品在法律上屬於其人所有、管有或控制；不誠實，指行為人明知自己沒有權力取得該物品，卻仍然拿取。相反，如行為人有真誠的法理依據認為自己有權拿取，則不構成不誠實；意圖永久剝奪，指行為人在拿走物品時，沒打算把東西歸還物主。即使後來被發現或心生悔意，只要當下有此意圖，罪名已成立。

四大要素中，控方要在毫無合理疑點下證明被告的內心世界有「不誠實意圖」，是最具挑戰的。如果被告

否認控罪，控方就必須要有足夠證據，方可令被告入罪。法庭一般會引用源自1982年英國《R訴Ghosh》案的測試準則：第一步（客觀標準）：根據普通、合理而誠實的一般常人標準，行為是否屬於不誠實？第二步（主觀標準）：被告當時是否自己意識到，以普通誠實人的標準，自己的行為是不誠實？若兩者答案皆「是」，即可裁定具不誠實意圖。

盜竊罪的成功抗辯，關鍵在於被告能否提出合理自辯。若被告真誠相信自己在法律上有權取得該財產；真誠相信若擁有人知道，亦定會同意，則在法律上不被視為「不誠實」。上述原則如套到該六合彩案，你認為案件的發展方向又會如何？