



「十五五」開局 香港如何擁抱AI?

鄧潔

近日「養龍蝦」在全球掀起熱潮，OpenClaw這款開源智能體正以驚人的速度滲透進我們的工作與生活。這場全民熱潮，究竟本質為何？可從以下四個層次理解：

技術門檻消解。OpenClaw將過去需要超長代碼才能實現的複雜操作，嵌入自然語言交互之中。從日常辦公再到生活場景，那些曾經只屬於專業人士的技術能力，正變得觸手可及。

生產力重構。智能體正在成為核心生產力單元，AI的角色正從「顧問」轉變為「數字員工」——它能像人一樣看螢幕、點滑鼠、敲鍵盤，完成從「打開軟件」到「輸出結果」的完整閉環。

應用場景競逐。科技競爭的焦點，正在從「誰的模型更完美」轉向「誰能率先在真實場景中跑通代理式AI」。科技巨頭們不僅比拼算力與參數，還拼誰能更快地在金融、政務、醫療、教育等垂直領域中，找到AI代理的落地場景，並形成可複製的解決方案。

信任邊界探索。熱潮的另一面，是技術「馴化」的緊迫命題。當智能體的安全問題開始浮現，例如「『龍蝦』無視『主人』叫停，執意刪除系統檔案」「智能體擅自轉賬給陌生人」，我們必須正視OpenClaw在預設或不當設置下可能存在的安全隱患。

技術普惠，必須伴隨安全邊界的清晰界定。這場「養龍蝦熱」恰恰為我們思考香港在「十五五」開局之年如何主動作為，提供了切入點。

打造「AI+金融」試驗點

「十五五」規劃提出加快高水平科技自立自強，深化拓展「人工智能+」。行政長官李家超強調，香港必須主動對接國家戰略，在「十五五」規劃中找準定位、積極作為。那麼，面對這場AI重塑浪潮，香港具體可以做一些什麼？

第一，發揮金融中心優勢，打造國家級AI金融應用試驗區。

香港作為國際金融中心，擁有高度發達的銀行、保險、資產管理、證券交易等

服務體系。這些領域資料密集、流程規範、監管嚴格，恰恰是AI智能體發揮價值的最佳試驗場。香港可成為「人工智能+金融」的試驗點。一方面，依託金管局的金融科技監管沙盒，為AI應用提供合規測試空間；另一方面，探索建立AI金融應用的行業標準，為內地金融機構的智能化轉型提供「香港方案」。

第二，發揮貿易樞紐優勢，建設AI驅動的智能物流中心。

作為國際貿易和航運中心，香港是擁有高效的通關體系和成熟的物流基礎設施。一份跨境貿易合同涉及報關、報檢、外匯結算、信用證審核等多個環節，AI智能體可以自動提取關鍵資訊、匹配貿易條款、識別潛在風險。

香港可主動布局，將自身打造為「AI+供應鏈」的區域樞紐。具體而言，依託企業的機器人倉儲網絡，推動貿易全鏈條的智能化改造；聯合深圳前海、廣州南沙等平台，構建大灣區統一的AI貿易服務平台；探索利用AI優化空港、海港的調度效率，鞏固香港國際航運樞紐地位。

第三，發揮專業服務優勢，構建AI賦能的高端服務業集群。

香港擁有大量高水平的法律、會計、諮詢、建築設計等專業服務機構。這些行業的共同特點是：人才成本高、重複性工作多、對精準度要求極高。以法律行業為例，一份跨境併購合同可能長達數百頁，AI智能體可以自動完成合同條款比對、案例檢索、合規性初篩，讓律師從繁瑣的文書工作中解放出來，專注於高價值的策略判斷。

香港可主動作為，推動專業服務領域的AI賦能。一是支援本地專業機構引入AI工具，提升服務效率與質量；二是鼓勵開發針對專業服務場景的AI應用；三是聯合內地城市，探索制定AI專業服務的跨境互認標準，將香港的高端服務能力輻射整個大灣區。

探索AI治理「香港方案」

第四，發揮制度獨特優勢，探索AI治理的「香港方案」。

當AI擁有了操控電腦、瀏覽重要檔案

的權限時，安全風險也隨之浮現。工信部連續發布安全預警，指出智能體可能存在指令誘導、資訊洩露和系統受控等風險。如何防止「越權瀏覽」？如何抵禦「惡意提示詞注入」？

香港的獨特價值在於能夠為這些難題探索答案。憑藉「一國兩制」下的制度優勢和普通法，香港可在資料跨境流動、知識產權保護、AI倫理規範等方面先行先試。香港可以主動作為，探索建立既符合國家要求、又能被國際認可的AI治理方案——這本身就是一種核心競爭力，也是香港為國家AI戰略作出的獨特貢獻。

對於香港而言，這場AI浪潮的核心機遇：不僅僅作為「超級聯繫人」，而是成為「創新轉化器」和「場景孵化器」。在AI從「技術炫技」走向「價值創造」的關鍵階段，香港的每一個優勢場景都對應着真實的需求和無限的想像力。主動作為，創造機會。以場景為牽引、以制度為優勢、以合作為路徑，香港在AI浪潮中全速前進，未來可期。

香港青年時事評論員協會成員

築牢私隱防線 促進AI安全發展

鍾麗玲

隨着人工智能（AI）生成內容的技術日趨普及和成熟，AI生成內容隨處可見。或許大家也看過AI生成的廣告短片、AI微短劇，或者由AI主播主持的節目等等，片中「人」的外表以至聲線都相當逼真。正因為AI深度偽造（深偽）技術能夠生成以假亂真的圖像、音訊及影像，一旦相關生成內容被不法分子用作網絡欺凌、詐騙，或製作未經當事人同意的私密影像，可能對受影響人士，尤其是兒童及青少年，造成嚴重傷害。

AI生成真人「脫衣」影像 觸發全球關注

最近一宗轟動全球的事故突顯這問題的嚴重性。有報道指，某個AI聊天機械人容許用戶上傳真實人士，包括兒童及婦女的照片，再透過指令（prompting）將相中人「脫衣」，在未獲當事人同意下生成私密影像。在短短11天內，該聊天機械人據報已生成約300萬張私密影像，可見AI技術能輕易被「武器化」，導致個人資料被大規模濫用。

事件曝光後，世界各地的私隱或資料保障機構迅速採取跟進行動，一些司法管轄區更對相關聊天機械人實施禁令。

事實上，AI的私隱風險近年來廣受全球監管機構關注，而個人資料私隱專員公署（私隱專員公署）亦一直積極與國際夥伴攜手合作，推動AI的安全發展。

在2025年9月舉行的第47屆環球私隱議會年會會議上，筆者聯同全球19個私隱或資料保障機構的專員或高級代表，簽署《建立值得信賴的數據治理框架以促進創新和保障私隱的人工智能發展聯合聲明》，倡議在AI系統的設計階段融入資料保障原則，建立穩健的數據管治機制。

其後，在今年2月，私隱專員公署與全球60個私隱或資料保障機構共同發布《AI生成影像及私隱保障聯合聲明》，提醒開發及使用AI內容生成系統的機構必須遵守適用的資料保障及私隱法例，並採取一系列措施保障資料當事人，尤其是兒童及弱勢群體的基本權益。

AI智能體帶來新挑戰

近期興起的AI智能體（Agentic AI）進一步加劇了AI的私隱及網絡安全風險。與一般AI聊天機械人相比，AI智能體擁有較高權限，能夠存取用戶裝置的檔案、連接外部工具及服務，並可代替用戶自主執行多步驟任務。正因AI智能體能夠以前所未有的速度和規模，存取、處理及披露個人資料，假如這些工具遭到濫用或系統遭到黑客控制，所帶來的私隱與安全威脅可想而知。

科技發展日新月異，令人鼓舞的是，行政長官在2025年施政報告已經提出，由律政司成立跨部門工作小組，協調負責的政策局檢視相關法律配套，配合本港更廣泛應用AI的發展和需要。

在此，筆者想強調，無論AI技術如何演變，只要過程中牽涉收集和使用個人資料，即受現行的《個人資料（私隱）條例》（《私隱條例》）規管。例如，未經他人同意下使用其影像製作及／或發布深偽內容，可能違反《私隱條例》的規定。惡意使用深偽技術更可能觸犯《私隱條例》下的「起底」罪行，甚至干犯其他刑事罪行。因此，所有持份者，包括AI開發者、服務供應商及用戶，必須正視創新技術可能帶來的風險，並負起責任及合法地開發或使用AI。例如，公署的指引建議機構在製作AI生成內容時，為相關內容加上標識或水印，以顯示內容由AI生成，避免造成混淆及誤解。

此外，若AI智能體導致個人資料被

未經授權或意外地查閱、處理、刪除、喪失或使用，亦可能違反《私隱條例》有關資料保安的要求。因此，公署建議，用戶應從官方渠道下載AI智能體的最新版本、按「最小權限原則」設定其存取權限，以及採取足夠措施確保系統安全及資料安全。用戶亦應持續評估相關風險，並且在要求AI智能體執行高風險操作時提高警惕，畢竟這些工具可以在轉眼間將用戶所有資料刪除或誤用。

堅持統籌發展和安全

國家「十五五」規劃強調，堅持統籌發展和安全。在發展中固安全，在安全中謀發展。在人工智能範疇，「十五五」規劃一方面提出全面實施「人工智能+」行動，另一方面又提到要加強人工智能治理，營造有益、安全、公平的發展環境。為進一步推進人工智能發展，行政長官在施政報告中明確提出，AI發展須以安全為舵，以應用為帆。

在追趕AI熱潮的同時，我們應積極主動對接「十五五」規劃，堅持統籌發展和安全的原則，有效防範化解各類風險。當中包括在開發或部署AI系統的初期，就已經要以保障個人資料私隱為核心標準，落實「貫徹私隱的設計」（privacy by design）及「預設私隱」（privacy by default）等原則，從而將侵犯私隱的風險降至最低。

近期事件揭示用戶，尤其是兒童及青少年在AI時代面對的風險不可忽視，而濫用或惡意使用AI可帶來深遠傷害。發展或應用AI的機構應引以為鑒，不應為追求新功能或加快推出新產品，而犧牲私隱和安全。所有持份者，包括AI開發商、服務提供者及用戶都有不可推卸的責任，為我們的下一代營造一個有益、安全以及公平的數碼環境。

個人資料私隱專員

加快建設國際人才集聚高地

郭王林 鄧錫綸 傑淇

智庫說

全國兩會圓滿閉幕，國家「十五五」規劃明確支持香港鞏固提升競爭優勢，建設國際創新科技中心，打造國際高端人才集聚高地。

發展之本在人才，試想若無源源不絕的人才供給，又談何「十大中心」「兩大樞紐」「一個生態圈」的戰略定位？面對經濟轉型、AI衝擊勞動市場及國際競爭加劇等多重挑戰，打造國際高端人才集聚高地不僅是國家對香港的殷切期許，更是香港自身可持續發展的關鍵。

建設人才高地需引才與育才並重，香港憑藉優質高等教育及國際化環境，本已具備吸引全球人才的優勢；然而，在全球人才爭奪戰及科技產業變革中，人才結構與技能必須與時俱進、同時緊扣未來產業需求，這才是建設人才高地的核心。

新一份財政預算案以「AI+」為主軸之一，推動全民AI培訓，呼應國家戰略，是香港搶佔科技先機重要的一步。要將這些舉措轉化為長遠人才發展的基石，香港一方面應深化「政產學研投」合作，培育創新領軍人才；另一方面推進全民數字賦能以革新勞動力技能，共同把握「AI+」時代機遇。

實現「政產學研投」協同效應

北部都會區是香港融入和服務國家發展大局的重要平台，也是深化「政產學研投」協同合作的載體。政府計劃透過北都大學城釋放土地供院校擴展，不僅能夠擴大高等教育容量，更應藉此強化政府引導、產業需求、學術研究、科研創新及投資聯動的機制。大學城應聚焦AI、生命健康、金融科技、先進材料

及新能源等國家重點產業領域，並引入海內外頂尖院校與企業設立聯合項目、實驗室及孵化器；同時，加強與新田科技城等創科園區的聯繫，形成「教育—科技—人才」一體化生態。如此，香港的基礎研究實力才能精準對接國家現代化產業體系，吸引全球英才匯聚，真正實現「政產學研投」協同效應，為香港的發展定位提供人才支撐。

預算案提出將僱員再培訓局升格為技能提升局，以加速現有勞動力的轉型，推動全民數字賦能。在AI正在重塑產業結構之際，技能提升局的使命不在於將人人變成AI專家，而是確保各行業從業人員掌握AI應用基礎，從容應對產業變革。上述轉變同時呼應「十五五」規劃提出「全方位推進數智技術賦能，促進實體經濟和數字經濟深度融合」的目標。

相關部門應前瞻分析香港產業的未來技能需求，識別AI時代的職位變遷，如哪些工作容易被自動化取代，哪些新技能（如人機協作、數據解讀）將成為必需等。培訓應分層進行設計，面對普羅大眾，應強調AI素養及實用工具；面對專業人士，則聚焦行業的應用，包括AI風險評估或物聯網數據分析等。透過與產業深度對接的針對性課程，將能為香港注入適應時代的勞動力，助力國家激活數據要素潛能、加快數智技術創新。

「十五五」規劃支持香港打造國際高端人才集聚高地，既是對香港獨特地位的肯定，亦是對未來發展的鞭策。透過深化「政產學研投」合作，賦能全民技能提升，香港必將能以自身所長，更好地融入和服務國家發展大局。

團結香港基金副研究總監、團結香港基金研究經理、團結香港基金研究員

伊朗將是特朗普的第三次失敗？

宋魯鄭

特朗普重返白宮後，憑藉第一任期積累的經驗和建立的唯他馬首是瞻的團隊迅速在全球兌現他的「美國優先」理念。不僅大打貿易戰，還肆意對聯合國會員國作出威脅或者動用武力。

由於種種原因，特朗普多數獲得了巨大成功。但也遭遇了兩次失敗。一是和中國的貿易戰。二是吞併格陵蘭島。

中美貿易戰打了一個月就結束，特朗普不得不和中國簽訂休戰協定。格陵蘭島則遇到了歐洲的強烈抵抗而不得不暫時偃旗息鼓。然而，面對兩次失敗的特朗普似乎並沒有汲取教訓，依然在舊的邏輯和軌道上前行，標誌性事件就是發動規模空前的美以伊戰爭。然而種種因素分析，伊朗很有可能成為特朗普第三個「麥城」。

首先從戰略戰術上來講就顯示了特朗普對伊朗的誤判。

開戰當天美國就取得驚人的斬首戰果。然而，出乎特朗普預料的是，這不但絲毫沒有影響伊朗的軍事反擊和國內政治運作，而且他所期待的民眾「起義」也沒有發生。

反而極其堅定了伊朗毫不妥協的對抗。

這個結果凸顯特朗普及其團隊對伊朗的不了解和誤判，把伊朗當作利比亞或者委內瑞拉。利比亞最突出的政治特點是卡扎菲執政以來就搞去國家制度化，一切依賴於個人。所以一旦他垮台國家政權立即崩潰，陷入無政府、軍閥割據狀態。委內瑞拉則是國家太弱小，美國可以隨時抓捕任何不合作的領導人，有着強大的威懾力。

但伊朗有兩點不同。一是它擁有九千萬人且具有相當強大的軍事能力。不僅曾和伊拉克打過八年戰爭，更重要的是自革命以來就面臨以色列和美國的威脅，雙方一再發生軍事衝突。其實際作戰能力和經驗均得到持續的檢驗和鍛煉。二是伊朗作為共和體制，政治制度化非常高，體制並不依賴某一個人而運作。而且面臨美的威脅早就進行去中央化的部署。所以哈梅內伊死亡後，第二天就通過體制產生了新的領導人，絲毫沒有影響對美的反擊。

其次，特朗普還是低估了伊朗以及這場衝突可能產生的後果。

伊朗的反擊不僅涵蓋了以色列以及美國在中東的所有軍事基地，而且第一次把

美國軍事實力的象徵航空母艦當作攻擊目標。甚至當英國同意美國使用其印度洋基地時，伊朗立即對英國在塞浦路斯的軍事基地發起攻擊。此外，伊朗立即封鎖霍爾木茲海峽，並多次攻擊經過海峽的油輪。宣稱不讓一滴油通過，要將世界油價打到200美元一桶。這都是前所未有的舉動，體現了伊朗破釜沉舟的決心。特朗普為此不得不修正開戰之初只打四天的計劃改為四周甚至更長，也首度表示要派地面部隊。

其後果立即在股市和油價顯示出來：道瓊斯指數最高一天下跌1200點，油價上漲超過80美元，並隨着戰爭的延續而繼續上漲。美國的經濟支柱主要是金融。政治穩定或者要想贏得選舉則主要依靠低物價。對伊開戰都直接影響到這兩個核心。戰爭從來不僅僅是絕對國力的檢驗還有戰爭意志和對後果的承擔能力。伊朗是生死存亡一戰，只能置於死地而後生。但美國卻不是。伊朗就是要通過持久戰拖出勝負。

第三，除了美以，沒有一個國家希望伊朗失敗。這當然不是得道多助，失道寡助的套話，而是切實利益使然。

中東各伊斯蘭國家雖然和伊朗有着宗

教和地緣衝突，但並不希望伊朗垮台。一是美國之所以和這些中東國家維持盟友關係，除了石油就是要對抗伊朗。實力遠居中東首位的以色列之所以願意和它們維持良好關係，很大的原因也是因為伊朗。如果伊朗被除掉，它們的戰略價值就喪失了。它們也深知，假如伊朗戰敗，下一個目標就可能是它們。從它們的角度，只要以色列在，伊朗就有存在的必要。所謂養寇自重就是此意。

而且很重要的一點，在這些中東國家看來，以色列和伊朗都是異己力量，和它們都有着重大利益衝突，因此非常樂見這兩個國家相互對抗和消耗。

二是這些中東國家和以色列媾和也是在懸殊的實力對比前提下為了生存而迫不得已，其內心中對以色列的仇視一直存在。以色列也心知肚明。從民族感情來講，它們認同伊朗對以色列的報復。從執政穩定來講，反以民意也不能忽視。

歐洲同樣不希望美國獲勝。原因簡單：伊朗不是歐洲的威脅，但特朗普治下的美國是。雖然歐洲也反對伊朗，但美國的做法是對國際秩序的嚴重破壞和衝擊。這也

是今天歐美之間最大的分歧和對抗的焦點。假如伊朗獲勝，不僅使得特朗普有所收斂，也會影響美國的中期選舉。歐洲可謂苦特朗普久矣。它特別希望美國國內能有力進行制衡，當下唯一的希望就是中期選舉。否則，特朗普勝利之下再贏取中期選舉，未來三年還不知道會做出什麼威脅歐洲和世界的舉動，例如再指向格陵蘭島。

事實上，伊朗如獲勝，將和中國反擊美國貿易戰、歐洲成功保衛格陵蘭島一樣，發揮維護國際秩序的作用。中國和俄羅斯也是一樣。一是中俄和伊朗關係良好，合作深廣，也都是上合組織和金磚成員國。二是面對美西方的遏制，伊朗一直都有牽制作用。從經濟和戰略層面，伊朗都不可或缺。至於廣大的南方國家更是長期以來不滿西方的雙重標準和霸道，這在俄烏衝突時表現得淋漓盡致。

總之，美伊之間的戰爭大概率會一直拖下去，客觀上發揮了制衡特朗普的作用。但中東的千年和平難題則不會消失，只會不斷延續存在。

旅法政治學者、復旦大學中國研究院研究員