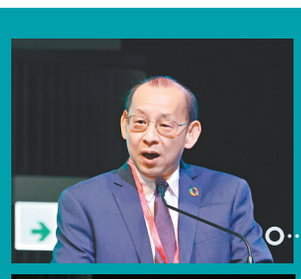
數碼港首合辦數字世界大會 與5大專院校簽備忘

WDTA籌建研究院 助港育AI人才

新一份財政預算案部署將香港發展為人工智能（AI）產業國際交流協作匯聚地。香港數碼港首次聯同國際組織世界數字科學院（WDTA）及國際院士科創中心（IASTIC）昨日合辦「數字世界大會：人工智能安全、可信、負責任」論壇，三方在會上簽署合作備忘錄，以攜手推廣 AI STR（安全、可信與負責任）測試和評估的最佳實踐，積極培訓AI人才及探索合作開發AI測試基礎設施。論壇期間WDTA宣布於數碼港籌建「世界數字科學亞太研究院」（亞太研究院），數碼港亦與五間本地大專院校簽署合作備忘錄，共同促進與AI相關的應用研究和人才培育，助力香港開拓AI新賽道。 ●香港文匯報記者 馬翠媚

▲全球人工智能行動峰會昨日舉行合作備忘錄簽署儀式。 香港文匯報記者萬霜靈 攝



世界數字科學院執行理事長李雨航
「AI發展必須以人為本、安全為基。」

國際院士科創中心創辦人陳清泉
「香港作為連接全球的創新樞紐，是推動AI治理與合作的理想平台。」

數碼港主席陳細明
「數碼港過去一年在構建人工智能生態圈方面取得顯著的成績。」

香港文匯報記者萬霜靈 攝

數字世界大會論壇達成的合作撮要

WDTA宣布於數碼港籌建亞太研究院

- 着力推動區內AI安全標準及相關舉措的制定
- 推動數字技術創新、培育科學與產業應用人才
- 促進數字時代的全球合作

數碼港與WDTA及IASTIC簽署合作備忘錄

- 攜手推廣 AI STR（安全、可信與負責任）測試和評估的最佳實踐
- 積極培訓 AI 人才及探索合作開發 AI 測試基礎設施

數碼港與五間本地大專院校簽署合作備忘錄（港大、城大、都會大學、香港高等教育科技學院、香港資訊科技學院）

- 共同促進與AI相關的應用研究和人才培育
- 為合作的大專院校學生提供實習及就業機會
- 為香港AI產業發展注入更多生力軍，促進本地AI發展

整理：記者 馬翠媚

WDTA昨表示，於數碼港籌建的亞太研究院，將着力推動區內AI安全標準及相關舉措的制定，推動數字技術創新、培育科學與產業應用人才，及促進數字時代的全球合作。WDTA是於2023年在聯合國框架指導下創立的國際新型創新和研究機構，旨在推動國際社會在數字技術領域的突破性進展，並致力構建一個更加安全、高效、共用的全球數字生態，而WDTA亦已發布三項AI STR標準，包括生成式人工智能應用安全測試標準、大語言模型安全測試方法和大模型供應鏈安全要求。

為大專生提供實習機會

除了推廣負責任的AI應用外，在培育人才方面，數碼港昨與五間本地大專院校包括香港大學、城市大學、都會大學、香港高等教育科技學院及香港資訊科技學院，在論壇上簽署合作備忘錄，共同促進與AI相關的應用研究和人才培育，例如為合作的大專院校學生提供實習及就業機會，藉以為香港AI產業發展注入更多生力軍，促進本地AI發展。另外，WDTA亦發布兩項AI人才認證課程，包括「大模型應用工程師認證（LLMAE）」與「大模型技術專家認證（LLMTE）」，旨在加速培育兼具技術實力與社會責任的下一代AI專業人才，推動AI安全、可信與負責任的發展。

世界數字科學院執行理事長李雨航昨出席論壇致辭時表示，AI發展必須以人為本、安全為基，他提出三項核心倡議：首先，構建「安全原生」的技術基因，將安全嵌入AI全生命周期，推動演算法透明度與數據溯源認證體系；其次，建立「以人為本」的價值坐標，讓技術服務於醫療普惠、中小企轉型等社會需求；最後，WDTA 實行「負責任創新」的全球承諾，其人工智能委員會在聯合國可持續發展目標指導框架下應對深度偽造、數據濫用等挑戰。

聯動標準制定 加速成果轉化

國際院士科創中心創辦人陳清泉出席同一場合時表示，香港作為連接全球的創新樞紐，是推動AI治理與合作的理想平台。他認為WDTA將以「速度、安全、共用」為核心原則，通過 WDTA亞太研究院加速聯動亞太地區政產各界在數字技術標準制定與前沿成果轉化，率先落地AI STR（安全、可信與負責任）的標準與測評認證體系，健全國際AI治理與安全體系。他強調唯有跨行業、跨國界的協作，才能實現「不讓任何人掉隊」的包容性數字未來。

「數字世界大會：人工智能安全、可信、負責任」論壇昨在數碼港舉行，出席嘉賓包括創科局局長孫東、中央政府駐港聯絡辦教育科技部副部長葉水球、數碼港行政總裁鄭松岩等，論壇亦邀請了不同學者、專家及來自公共行政、金融、醫療等行業領袖，就「跨行業AI轉型」及「平衡AI創新應用與風險」等多個有關與AI應用相關熱門議題，例如如何在不同領域中善用AI提高效率、改善服務質素及應對新挑戰等，就不同議題分享見解和實務經驗，吸引了不少關注AI發展、數字技術創新的人士參與，現場所見活動座無虛席。

聚350 AI及大數據企業 數碼港建港AI生態圈

香港文匯報訊（記者 馬翠媚）數碼港首次聯同國際組織世界數字科學院（WDTA）及國際院士科創中心（IASTIC），合辦「數字世界大會：人工智能安全、可信、負責任」論壇，昨在數碼港舉行，此為剛於法國巴黎結束的第三屆「全球人工智能行動峰會」的香港分會場。

超算中心及實驗室投入服務

數碼港主席陳細明在致辭時表示，作為香港的數碼科技旗艦及人工智能加速器，數碼港過去一年在構建人工智能生態圈方面取得顯著的成績，包括已投入服務、香港目前規模最大的數碼港人工智能超算中心，及數碼港人工智能實驗室，集結本地人工智能生態夥伴企業及人才，促進相關技術的研發及合作，他期待繼續與各界合作，推動完善香港的人工智能生態圈，及人工智能的「向善」發展。

他提到，數碼港現時匯聚逾350間專注研發人工智能及大數據的初創企業，並且引進多家人工智能領軍企業，結合他們在算力開發、大模型建設、演算法、數據科學等研發能力，促進人工智能研發創新及應用。

人工智能資助計劃已批5項目

數碼港人工智能超算中心以及人工智能實驗室已於去年底投入服務，透過匯聚內地及海外人才及創新資源，在人工智能生態鏈的不同環節支持創新研發及應用，推動產業化發展，同時數碼港亦獲政府撥款30億元，推行為期3年的「人工智能資助計劃」，用作資助本地院校、研發機構及企業等善用超算中心的算力，提升研發能力、推動科研突破，加速創科產業化發展。計劃去年10月起接受申請，財政司司長陳茂波日前披露，已批准5個由本地大學、科研機構等牽頭的項目，加速推動本地與大語言模型、新材料、合成生物學大模型等相關的研發工作。

數碼港有軟硬件技術 助企業安全用AI

香港文匯報訊（記者 黎梓田）全球人工智能（AI）發展迅速，香港新一份財政預算案，有頗多關於加快香港人工智能發展的措施，數碼港行政總裁鄭松岩昨在全球人工智能行動峰會上致辭表示，數碼港內與人工智能及數據科學有關的公司超過120間，能為企業提供技術解決方案，將積極與海外大學、研究機構及監管機構合作，推動建設一個安全、可信、負責任的人工智能生態。

企業層面應用仍然較少

鄭松岩表示，目前許多企業和機構雖然都熱切期望利用人工智能提升效率、降低成本，或進行親民的創新，但實際上，香港真正成功將人工智能模型融入企業日常運作流程的案例仍然很少。個人層面的應用較多，但企業層面應用仍較少。

他認為原因有二。首先，是企業對人工智能技術及其應用的專業人才仍然不足，因此許多企業對於是否及如何應用人工智能仍持猶豫態度，擔心不知道選擇哪種技術或工具。其次，企業對人工智能應用的風險也存在疑慮。他們擔心使用人工智能可能帶來一些風險，尤其是將其融入運營流程後，特別是在一些對風險要求較為嚴格的行業，如銀行業，他們會有很多顧慮。

●數碼港行政總裁鄭松岩

鄭松岩表示，作為香港數字科技的樞紐和人工智能的加速器，數碼港致力於建設人工智能生態，協助各行各業盡早掌握人工智能的應用。數碼港構建的人工智能生態包括硬件、人工智能基礎大模型、行業數據模型、海內外人工智能應用工具，以及相關解決方案。因此，如果企業不確定如何應用人工智能，可以嘗試尋求數碼港提供的技術解決方案。

逾百AI公司對接不同行業

他提到，除了硬件支持和技術方案外，數碼港還提供實際應用的案例。過去一年，數碼港內與人工智能及數據科學有關的公司超過120間，這些公司因其產品對接不同行業，累積了大量行業應用案例。數碼港相信，企業可以從中受益。同時，數碼港除了提供技術解決方案外，還組織了關於人工智能的倫理、風險管控等方面的研究。

他表示，數碼港希望通過這些努力，協助企業管理人工智能帶來的風險，減輕對用戶的不利影響，並確保業務在意外發生時的持續性。數碼港亦將積極與海外大學、研究機構及監管機構合作，推動建設一個安全、可信、負責任的人工智能生態。

螞蟻張天翼：AI技術越提升 錯誤越難發現

香港文匯報訊（記者 黎梓田）人工智能（AI）技術近年呈現爆發式發展，其在企業及人們生活中的應用也越來越廣泛，但其安全及風險仍是關注重點。螞蟻國際風險管理部總經理張天翼昨在全球人工智能行動峰會上表示，人工智能風險一般主要包括三類：內生安全、服務安全和衍生安全。關於人工智能的內生安全，大家可能比較熟悉的問題包括其價值觀問題和幻覺問題。過去一兩年，主要的大模型開發公司都在集中力量解決這類問題，特別是幻覺問題。但隨着基於檢索增強生成等更多檢索與推理方式的融合，發現人工智能的幻覺問題並未徹底消失，反而可能變得更加隱蔽。

他舉一個在春節期間使用某大模型的例子，「當時我用它為親戚家的小孩取名字，它非常快速地給出了許多引經據典的建議，其中三個名字是真的，兩個是假的。與幾年前大模型剛出現時的情況不同，以前的幻覺問題一眼就能識破，比如它聲稱某詩是杜甫或李白寫的，這是明顯錯誤。但現在它使用非常冷門的詩人和作品，編造了幾句詩，還保持了風格的一致性，並且同時進行連鎖推理和自證。如果是顯而易見的錯誤，它會在自證過程中被排除出去。因此，如果說幾年前人工智能的幻覺顯得笨拙，現在它的幻覺則變得更加狡猾。」

●螞蟻國際張天翼

第二類是與智能體相關的風險。隨着人工智能的湧現及躍升，它被應用於越來越多的場合。但在此過程中，也出現了更多預料中或預料外的風險。其中隱私是大家非常關注的問題，既看到在訓練過程中隱私數據可能被提取出來的情況，也發現了有針對性的攻擊。

生成技術衍生欺詐危機

第三部分是衍生安全，即利用生成式人工智能（AIGC）的能力，生成出大家已廣泛看到的圖像、視頻生成等功能。在這方面，已在反欺詐領域看到了非常現實的危害。例如之前擔心的問題——比如批量生成偽造的身份證，用來篡改或冒認身份——在金融實踐中已經發生了大量案例。這意味着人工智能門檻的降低、成本的降低及其可達性的增強，確實大大增加了這些風險。

「以AI對抗AI」提升防禦

張天翼又表示，螞蟻集團過去幾年內開發的，針對這些人工智能應用安全問題的應對措施，總體來看，集團從攻擊與防禦兩個方面進行了強化。首先，所謂「攻擊」是指希望模擬人工智能，通過「以AI對抗AI」(AI against AI)的思路，提升其評測能力，發現可能的風險所在。然後利用人工智能能力提升其自身的防禦技術，包括上述提到的內生安全、衍生安全和服務安全。

投推署湖北推介港供應鏈管理優勢

香港文匯報訊（記者 歐陽思柔、張帥 武漢報道）香港特區政府新一份財政預算案提出香港建設「跨國供應鏈管理中心」，香港特區政府投資推廣署署長劉凱旋在湖北接受採訪時指，全球供應鏈正經歷重大轉型，香港作為唯一匯聚全球優勢和中國優勢的都市，是內地企業可以信賴的跨國供應鏈管理中心。

200企業代表參會 了解港優勢

劉凱旋2月26日至28日展開上任首次對湖北省武漢市的訪問，她此行是為向湖北政府部門、重點開發區及企業群體宣傳香港的營商新機遇，以及香港作為跨國供應鏈管理中心的優勢。26日，投資推廣署聯合中國國際貿易促進委員會湖北省委員會、湖北省商務廳、特區政府駐武漢經濟貿易辦事處及香港貿易發展局，在武漢市舉辦了「鄂港合作 鏈接全球」研討會，吸引湖北省本地逾200位企業、機構及傳媒代表參加。

劉凱旋對於發揮鄂港之間經貿投資優勢、促進企業把握香港機遇成長升級充滿期待。她總結了香港在致力成為跨國供應鏈管理中心方面具備的優勢。她指出，全球供應鏈正經歷生產基地多元化、供應網絡區域化和關鍵產業在地化等重大轉型，在新格局下，「跨國供應鏈管理中心」的需求應運而生。而香港在「一國兩制」下，憑藉其優質營商環境，包括豐富的對外貿易經驗、高質量專業服務、高素質人才資本，配套完善的港口、機場和其他基礎設施，以及可靠的貿易融資選擇，能在企業採購、貿易、物流、技術、金融等多個領域提供一站式服務，是世界上唯一匯聚全球優勢和中國優勢的地方，能夠成為內地企業可信可靠的跨國供應鏈管理中心。

來港開設管理離岸貿易總部

劉凱旋表示，投資推廣署希望吸引內地生產企業來港開設管理離岸貿易總部，讓企業以香港為基地，管理跨國供應鏈的運作流程。

●投資推廣署署長劉凱旋指，香港是內地企業可以信賴的跨國供應鏈管理中心。 香港文匯報記者歐陽思柔 攝

特區政府駐武漢辦主任蔡敏君接受採訪時表示，供應鏈、資金鏈是香港的強項，在國際化市場、全球物流、資金流通等方面，一直保持全球領先的地位，這對於內地企業走向全球是非常重要的。