專家：升級安全體系 研設人工智能體「白名單」

增衛士加護欄 消除AI「養龍蝦」隱患

俗稱「龍蝦」的AI智能體OpenClaw近期異常火爆，國內主流雲平台均提供了一鍵部署服務。多位參加全國兩會的代表、委員提醒，該款AI智能體執行能力強大，既能成為優秀的「數字員工」，也會給「養蝦人」帶來安全挑戰。

「AI智能體是一個新物種，聰明程度已不亞於人類，傳統的安全軟件已經對付不了它。」全國政協委員、360集團創始人周鴻禕對《大公報》透露，在安全保護上，以前的安全掃描軟件對這類AI新物種已有些力不從「新」。代表委員建議，未來需要開發出新的Agent（智能體）衛士，去進行漏洞處置和攻擊溯源分析。此外可以考慮設立AI智能體安全「白名單」，只允許名單內的對象運行服務，讓用戶能夠安心使用智能體。

大公報記者 張帥北京報道

◀3月11日，在雲南省騰沖市一家手機專賣店內，工作人員在和同伴交流開源AI智能體「龍蝦」的操作體驗。 新華社

OpenClaw憑自然語言指令自主執行文件管理、郵件收發、數據處理等複雜任務，但為實現「自主執行」，該應用需授予極高系統權限，包括訪問本地文件、讀取環境變量等。近日工信部及中國國家互聯網應急中心（CNCERT）接連發布公告，警示用戶留意「龍蝦」存在的嚴重安全隱患，並建議企業及個人用戶採取多項防護措施。

「沒有安全的創新走不遠」

對於OpenClaw的具體安全風險，中國信息通信研究院副院長魏亮提醒，OpenClaw在調用大語言模型的時候可能誤解用戶指令內容，導致執行刪除等「有害」操作，若使用被植入惡意代碼的技能包，還可能導致數據洩露或系統受控。因為明文存儲密鑰等配置問題，即使升級到最新版本，如果不採取針對性的防範措施，依然存在被攻擊的風險。

「沒有安全的創新走不遠、走不穩，安全和創新並非對立，而是一體兩翼，為AI預設『安全護欄』至關重要。」全國政協委員、全國工商聯副主席、奇安信集團董事長齊向東表示，要順應「AI+」場景變革趨勢，加快推進網絡安全體系升級改造，築牢數字安全屏障。

周鴻禕指出，網絡攻防形態已從過去的「人和人」對抗升級為「人和機器」的不對稱對抗，AI自身風險逐步加劇，一旦與業務系統深度結合，可能帶來更複雜的安全隱患問題。安全行業亟需轉型，開發出新的Agent（智能體）衛士，去進行漏洞處置和攻擊溯源分析，保證「龍蝦」們在用戶電腦上不會破壞系統、不刪除數據、不洩露密碼等隱私信息。

AI平台企應履行風險評估義務

全國人大代表、中國工程院院士高文指出，OpenClaw等智能體工具的湧現極大降低了創業門檻，但其開源工具的屬性也懸置了安全責任。用戶需注意防範潛在的網絡安全風險，提供AI智能助手服務的互聯網平台企業也需壓實主體責任，履行安全風險評估等義務。

另有代表委員透過《大公報》表示，可以考慮設立AI智能體安全「白名單」（只允許名單內的對象運行服務），讓用戶能夠安心使用智能體。同時，加快人工智能相關專項立法，明確平台、開發者與用戶的安全邊界、權利義務及法律責任，構建權責清晰的AI安全治理體系。

▲3月11日，在中國（南京）軟件谷「質能・工坊」OPC社區，技術人員安裝完開源AI智能體「龍蝦」後與用戶（左）交流。 新華社

▲全國政協委員、360集團創始人周鴻禕。

▲全國政協委員、全國工商聯副主席、奇安信集團董事長齊向東。

防患未然

工信部列四應用場景 詳解「龍蝦越權」對策

針對OpenClaw應用中的安全風險，工業和信息化部網絡安全威脅和漏洞信息共享平台（NVDB）組織智能體提供商、漏洞收集平台運營單位、網絡安全企業等研究提出建議。3月11日，工信部公告列舉「龍蝦」四種不同典型應用場景下存在的安全風險，包括智能辦公場景供應鏈攻擊和企業內網滲透、開發運維場景系統設備敏感信息洩露和被劫持控制、個人助手場景個人信息被竊和敏感信息洩露、金融交易場景引發錯誤交易甚至賬戶被接管的突出風險等，並給出應對策略。

其中，在企業智能辦公場景下，用戶使用「龍蝦」時如引入異常插件、「技能包」等，會引發供應鏈攻擊。為防止類似情況發生，用戶應獨立網段部署，禁止在內部網絡使用未審批的「龍蝦」智能體終端。個人用戶通過即時通訊軟件等遠程接入本地化部署的「龍蝦」使用「個人助手」服務時，「龍蝦」權限過高，易產生惡意讀寫、刪除任意文件的狀況。在互聯網接入情況下，系統易遭受網絡攻擊入侵。用戶應加強權限管理，禁止訪問敏感目錄，禁止非必要互聯網訪問，嚴格通過加密方式存儲配置文件、個人重要信息等。

此外，工信部對於「龍蝦」給出「六要六不要」的安全使用建議，包括使用官方最新版本，嚴格控制互聯網暴露面，堅持最小權限原則，謹慎使用技能市場，防範社會工程學攻擊和瀏覽器劫持，同時建立長效防護機制。 綜合報道

安全使用「龍蝦」 六要六不要

使用官方最新版本

- 要從官方渠道下載最新穩定版本，並開啟自動更新提醒；在升級前備份數據，升級後重啟服務並驗證補丁是否生效。
- 不要使用第三方鏡像版本或歷史版本。

嚴格控制互聯網暴露面

- 要定期自查是否存在互聯網暴露情況，一旦發現立即下線整改。
- 不要將「龍蝦」智能體實例暴露到互聯網，確需互聯網訪問的可以使用SSH等加密通道，使用強密碼或證書、硬件密鑰等認證方式。

堅持最小權限原則

- 要根據業務需要授予完成任務必需的最小權限，對刪除文件、發送數據、修改系統配置等重要操作進行二次確認或人工審批。
- 不要在部署時使用管理員權限賬號。

謹慎使用技能市場

- 要審慎下載ClawHub「技能包」，並在安裝前審查技能包代碼。
- 不要使用要求「下載ZIP」、「執行shell腳本」或「輸入密碼」的技能包。

防範社會工程學攻擊和瀏覽器劫持

- 要使用瀏覽器沙箱、網頁過濾器等擴展阻止可疑腳本，遇到可疑行為立即斷開網關並重置密碼。
- 不要瀏覽來歷不明的網站、點擊陌生的網頁鏈接、讀取不可信文檔。

建立長效防護機制

- 要定期檢查並修補漏洞，及時處置可能存在的安全風險。
- 不要禁用詳細日誌審計功能。

在出境大廳見證開放的脈動

「五年規劃」與我

周鴻圖 開元周遊集團董事長、德國中國商會慕尼黑分會會長

對深耕出境旅遊行業的我而言，「十四五」規劃實施的五年，是我所在行業歷經起伏、浴火重生的五年，也是我最真切體會到「國家發展與個人事業同頻共振」的五年。

「十四五」初期，全球疫情突如其來，給出境旅遊行業帶來重創。航班停飛、邊境管控、簽證暫停，我第一次如此真切地感受到，國際人員往來的暢通不僅是一個行業的生存根基，更關乎無數家庭「走向世界」的期盼。困境中，「十四五」規劃中「高水平對外開放」「暢通國內國際雙循環」的部署，成了我和同仁堅守的底氣。我清楚，這些關鍵詞裏藏着行業復甦的希望。

隨着疫情防控形勢好轉，國家優化出入境政策、恢復國際航線、推出簽證便利化措施。我至今記得疫情後我們組織的首個法蘭克福出境團，一位年近六十的女士握着我的手說：「感覺像重新打開了世界。」這句話讓我看到了規劃落地的溫度。

這幾年，出入境政策持續優化，過境免簽範圍擴大、免稅政策完善，為行業注入動力。我們也從「有沒有團可做」的焦慮，轉向「做好高品質產品」的思考，某種意義上，旅遊已從單純的消費行為，轉變為連接中國與世界的重要橋樑。

2026年全國兩會召開，站在新五年的起點上，我更懂得「擴大高水平對外開放」「促進服務消費提質升級」的現實意義。宏觀政策的推進，最終都會落在微觀場景裏——落在機場的登機口，落在護照上的一個個出入境章，也落在無數家庭走向世界的腳步中。展望「十五五」，隨着兩會相關部署落地，我堅信出境旅遊會有更廣闊空間。

大公報記者任芳頡整理

◀周鴻圖堅信，隨着兩會相關部署落地，出境旅遊會有更廣闊空間。

服務有溫度 履職有力度

兩會零距離

3月11日上午，全國政協十四屆四次會議在人民大會堂圓滿閉幕。天安門廣場上，服務兩會的禮賓隊一曲活力滿滿的《立春》手勢舞翩躚綻放，引來與會委員和媒體記者紛紛駐足，為這場盛會增添了一抹溫暖的青春亮色。

「選擇〈立春〉手勢舞，契合萬物復甦的時節，將傳統節氣與兩會圓滿召開相融，寄託國泰民安、五穀豐登的美好祝願。」禮賓隊領隊趙紅英說，負責代表委員迎送引導、會場禮序、證件核驗等是他們禮賓隊的工作，每項工作都不可或缺，必須做到萬無一失。

每次到天安門廣場，總能看到禮賓隊姑娘們舉着引導牌的身影。記者了解到，舉引導牌，這看似簡單的動作，卻需要足夠的臂力支撐。高質量精準服務，背後是艱辛的訓練——姑娘們半小時一組，連續訓練7天以上，每日單舉引導牌練習便有一兩個小時。

兩會現場，像禮賓隊這樣專業精細的服務隨處可見：人民大會堂入口，「雙人一機」智能核驗高效便捷，一名工作人員細緻覆核信息，另一名則以規範手勢引導通行，盡顯貼心與專業；人民大會堂內的飲水處，綠茶、花茶、白開水永遠都是整齊地擺放，水溫低的紙杯總會在第一排……

而議事殿堂上，代表委員盡心履職，為了獲得高質量建議、議案提案，日常深入基層，傾聽民聲……全國政協委員江浩然兩會前還在武漢調研AI數據安全，駐地書桌擺滿調研筆記，3份提案字字務實，呼籲反對新質生產力「一刀切」，推動傳統與新興產業協同發展。

履職盡職的代表委員與專心專業的工作人員交相輝映，他們以高度的責任感和使命感，共同繪就了兩會中各盡其責、同心向國的動人篇章，奏響了屬於這個時代的奮進強音。

大公報記者于海江

▲在天安門廣場，禮賓隊一曲《立春》手勢舞翩躚綻放。 大公報記者于海江攝

「小家」看大會：連民心的好建議多多益善

記者手記

今年全國兩會圓滿完成各項議程後即將勝利閉幕。站在大會堂前，我突然想起前兩天家裏的一段對話。

兩會開始後的一天，我在家正遇到鐘點工阿姨上工，她見到我特別興奮，「哎呀，聽說今年兩會有代表說到彩禮問題了，建議彩禮少一點，這個代表真是太好了。」我知道阿姨家的孩子即將婚配，她正在為高額彩禮發愁，這可能是她聽到最開心的建議了。

聽到此，公公婆婆出來，高興地與阿姨說起今年兩會有好幾個代表建議提升農民養老金的事。公婆是地地道道的農民，他們在抖音上刷到了全國人大代表、山西基層幹部雷茂端的建議。很巧，他們跟雷代表是老鄉，也是山西運城人。

「這樣的代表真是好代表，也是我們農民的驕傲。」他們說得很熱鬧，也很興奮。公婆念叨着代表們的好——聽到好幾個人大代表建議把70歲農民養老金漲到500元，他們非常開心，甚至開始跟阿姨憧憬以後老了回村子裏種糧種菜，加上一共1000塊的養老金，日子應該很美好……

我一直很少與他們談工作，也總覺得全國兩會似乎離他們有點遠。但那天，看到他們三個在一起熱絡地聊兩會，我才發現，原來兩會就在老百姓身邊，在他們的柴米油鹽、三餐四季裏，而這些被「民眾點讚」的建議也承載着人民群眾最真實的認可。這時，我不由得想起那句話：每個「小家」熱氣騰騰，中國這個「大家」就蒸蒸日上。這樣接地氣連民心的好建議、議案提案，多多益善！ 大公報記者馬靜