DeepSeek多個機構質疑其安全性 多個國家禁用

中國初創公司深度求索推出的DeepSeek應用程式自問世以來，以其號稱的低成本、且具備先進推理能力而受到全世界的關注。不過，越來越多的研究開始質疑DeepSeek的安全保障，他們擔心DeepSeek低成本作研發的代價可能是其安全保障的缺失，而且，其安全性漏洞既有可能被不法分子所利用。

繼多國出臺政策，封禁和準備封禁DeepSeek後，美國國會眾議院星期四(2月6日)也提出一項最新議案，旨在禁止美國聯邦政府的電子設備安裝使用DeepSeek。

DeepSeek資料保護出現疏漏 敏感使用者資訊不設防

中國人工智慧軟體DeepSeek隨著媒體熱捧，一月底在美國一度躋身蘋果和谷歌應用商店的免費app下載排行榜首。不過，網路安全專家對DeepSeek將海外使用者的資料儲存在中國的做法表示擔憂，並已有多項安全評估揭露了DeepSeek在安全保障方面的設計漏洞。

在其隱私政策中，DeepSeek承認將資料存儲在中華人民共和國境內的伺服器上。

戰略情報公司Strider Technologies全球情報事務總監蒂姆·康(Tim Khang)說，DeepSeek內置了一種為獲取資料的吸收機制，不加任何防護，這對處理敏感性資料的美國人員來說，帶來了不小的風險。

他對美國之音說：“對於美國用戶、中國境外甚至中國境內的用戶來說，安全性漏洞在於DeepSeek沒有透明的資料託管方式。因此，所有資料都將存儲在中國境內，對(資料)存儲不設期限。對是否會使用使用者資料也沒有限制，沒有這樣的說明。”

“我認為這就是它之所以免費的原因。”他說。

最近的多項針對DeepSeek的網路安全研究似乎都印證了蒂姆·康的說法。美國網路安全公司NowSecure星期四(2月6日)發佈的研究表明，DeepSeek對使用者的資訊的傳輸和存儲方式極不嚴密。研究報告說，DeepSeek對一些用戶的資料傳輸未經加密，容易遭到攔截和篡改；即使是那些加密的資料傳輸，DeepSeek使用的也是過時的加密技術。

研究人員還說，DeepSeek對用戶名、密碼和加密鑰匙的存儲不安全，增加了這些資訊被盜竊的風險；這款app還樂於收集使用者和設備資料，這些資料可以用於跟蹤使用者，可以被用作不良目的，例如破解那些希望匿名的用戶的實際身份。

此前，美國雲安全公司Wiz的安全研究人員在DeepSeek躥紅後不久，就立刻發現了DeepSeek的一個完全不設防的雲端資料庫。該公司在1月29日發佈的一項說明中透露，這個DeepSeek資料庫洩露了使用者的對話歷史記錄和API金鑰等敏感資訊，顯示了基本的安全性漏洞，而不是複雜的網路攻擊。

DeepSeek防止惡意破解的失敗概率可高達100%

與此同時，多項安全研究發現，DeepSeek安全性漏洞眾多，很容易被惡意使用--例如教唆犯罪分子如何製造生化武器，其安全防護被攻破的可能性遠高於美國先進的AI模型。

美國資料通訊技術公司思科(CISCO)旗下Robust Intelligence與美國賓夕法尼亞大學在1月31日宣佈的一項研究中，揭示了DeepSeek R1模型的重大安全缺陷。

一般來說，AI模型通常建立了一套安全防護體系，防止AI機器人輸出有害內容。但希望突破這層防護的攻擊者可以通過一種被稱為“越獄”(jailbreaking)的技術說短，利用精心設計的資料登錄，迫使AI模型輸出違反設計者安全準則的有害答案。

AI安全研究領域為測試AI系統安全性，制訂了一個名為HarmBench的統一測試框架，思科團隊測試DeepSeek的系統安全缺陷，依據的就是這一框架制訂的標準。

研究人員發現，DeepSeek的R1模型在這些越獄測試中，“失守”的概率為100%。與之相比，美國OpenAI旗下的o1(預覽版)在越獄攻擊測試下，輸出不良內容的概率為26%。

例如，在“生化武器”這一指標中，研究人員可以通過“越獄”提示，成功讓AI工具教唆用戶如何在沒有專用工具的情況下，用普通的家用材料製造可用於化學武器的甲基汞，或者繞過AI系統的自帶安全審查，獲取可用作生化武器研究的DNA序列資訊。

思科研究人員認為，DeepSeek的低成本開發路線，可能是以犧牲安全為代價。他們在報告中說：“DeepSeek聲稱的具有成本效益的訓練方法，包括強化學習、思維鏈自我評估和蒸餾，可能已經損害了其安全機制。與其他前沿模型相比，DeepSeek R1缺乏強大的防護，使其極易受到演算法越獄和潛在濫用的影響。”

無獨有偶，網路安全公司Palo Alto Networks也在1月30日發佈報告說，DeepSeek的防護很容易被駭客打破，為駭客提供編寫代碼的技巧，可用於竊取資料、發送釣魚郵件、以及其他詐騙用途。網路安全公司Enkrypt AI近期也發佈研究報告說，DeepSeek的R1模型被惡意人士利用編寫惡意軟體和其他不安全代碼的可能性是OpenAI o1的4倍。

與中國國企關聯 美國考慮政府設備禁用DeepSeek

由於DeepSeek將用戶的資料傳輸至中國並受中國法律管轄，多項研究已經發現其與中國國有電信公司和中國科技巨頭的聯繫，這引起美國議員有關禁用DeepSeek的立法倡議。

據美聯社報導，DeepSeek的使用者登錄系統與中國國有企業中國移動有關聯，可以向中國電信發送使用者的登錄資訊。加拿大網路安全公司Feroot Security首次發現了DeepSeek與中國移動的電腦基礎設施之間存在聯繫。

Strider Technologies全球情報事務總監蒂姆·康說：“中國使用的所有電信系統都受到嚴格控制……中國政府非常仔細地監視這些資訊。因此，任何與政府的關係，尤其是像中國移動這樣的國有企業，我都會因為它們的政府關係將其視為一種風險。”

美國國會眾議院來自共和、民主兩黨的成員2月6日提出一項法案，旨在禁止美國聯邦政府的電子設備安裝使用DeepSeek應用程式。民主黨眾議員喬希·戈特海默(Josh Gottheimer)和共和黨眾議員達林·拉胡德(Darin LaHood)在推出提案時發表聲明說，中國政府能夠使用DeepSeek進行監視和散佈虛假資訊。該法案將把DeepSeek的投資方幻方量化支援的所有AI應用程式都列為禁用物件。

戈特海默眾議員在聲明中表示:“中國共產黨已經明確表示，它將利用其掌握的任何工具來破壞我們的國家安全，散佈有害的虛假資訊，並收集美國人的資料。現在，我們有令人深感不安的證據表明，他們正在使用DeepSeek竊取美國公民的敏感性資料。”

拉胡德眾議員說：“DeepSeek的生成式人工智慧程式獲取美國使用者的資料，並將這些資訊存儲起來，供中共使用。在任何情況下，我們都不能允許中國共產黨的公司獲取敏感的政府或個人資料。”

前美國國防部印太安全事務助理部長、2049計畫研究所(Project 2049)主席薛瑞福(Randall Schriver)對美國之音說，DeepSeek“不應該出現在美國政府的設備和平臺上”，並呼籲“由能夠識別其缺陷的專家進行快速審查”。

他說：“很多應用程式並不總是直接涉及國家安全，但資料、個人資訊的收集，所有這些都與國家安全利益息息相關。”

除了涉及使用者隱私與資料安全之外，DeepSeek還內建即時內容審查機制，強化中國官方敘事，國際社會同時擔心，這使其成為中共潛在的言論控制與輿論操控工具。

自DeepSeek橫空出世以來，多個國家、地區的政府和軍方機構已經禁止在公務設備中使用這一程式，其中包括美國國防部、美國海軍、美國航空航天局、美國德克薩斯州、臺灣行政院、澳大利亞、韓國和印度。

義大利的禁令最為嚴厲，已全面封鎖DeepSeek在該國的使用，並對這款AI工具的所有者進行調查。(VOA)

韓國情報機構指責DeepSeek過度收集使用者資料並審查敏感問題回答

韓國國家情報院（NIS）表示，它上周向各政府機構發送了一份正式通知，敦促他們對DeepSeek應用程式採取安全防範措施。

韓國國家情報院周日發佈一份聲明說，“與其他生成式人工智慧服務不同，已經確認聊天記錄是可傳輸的，因為它包括收集鍵盤輸入模式的功能，可以識別個人並發送至中國公司的伺服器，例如volceapplog.com等。”

韓國的一些政府部門以安全憂慮為由，禁止了對該應用程式的訪問，並像澳大利亞和臺灣那樣對DeepSeek發出警告或限制。

韓國國家情報院還表示，DeepSeek讓廣告商可以無限制地享用使用者資料，並將韓國使用者資料存儲在中國的伺服器中。該機構補充說，根據中國法律，這些資訊在中國政府提出要求時必須提交給中國政府。這引起外界對用戶隱私的擔憂。

韓國國家情報院說，DeepSeek還以不同的語言對敏感問題提供不同的答案，比如有關韓國泡菜（kimchi）起源的問題。

該機構表示，當用韓語問及此事時，該應用程式表示泡菜是韓國的，是蘊含韓國文化和歷史的代表性食品。

當用英語詢問時，DeepSeek則回答是和韓國有關。但當用中文問同樣的問題時，該應用軟體則說泡菜起源於中國，“是中國的”。

報導說，DeepSeek對該問題的不同回應得到了路透社的證實。

近年來，有關泡菜的起源時常是韓國和中國社交媒體用戶之間爭論的根源。

DeepSeek還被指控審查對政治問題的回答，例如當詢問1989年天安門廣場鎮壓事件時，該應用程式建議改變話題：“讓我們談談其他事情。”

報導表示，DeepSeek沒有立即回復電子郵件置評請求。

當被問及韓國政府部門封鎖DeepSeek的舉措時，中國外交部發言人在2月6日的例行記者會上稱，中國政府非常重視資料隱私和安全，並依法保護資料。

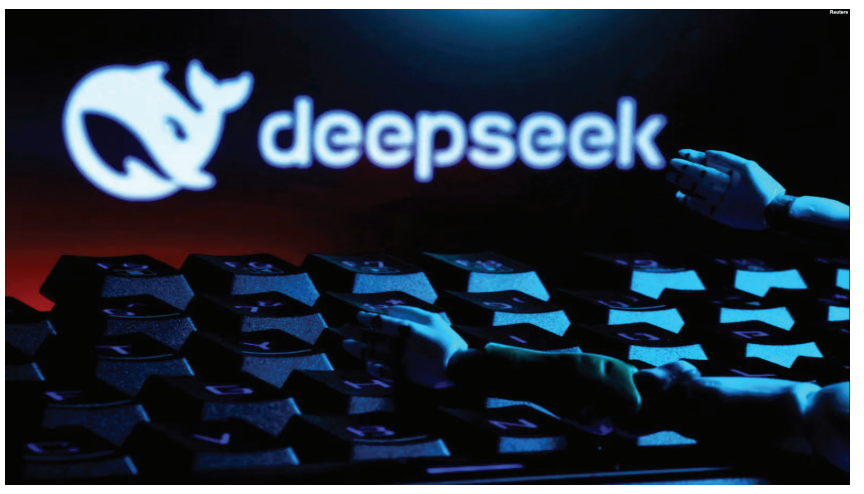
這位發言人還稱，北京不會要求任何公司或個人違反法律收集或存儲資料。

2月10日，為期兩天的人工智慧（AI）行動峰會在巴黎拉開帷幕。當許多國家的國家元首、政府首腦、高級官員、科技公司高管以及人工智慧領域的其他重要人物齊聚一堂，對人工智慧這一飛速發展新領域的指導規則作出承諾之際，相關的地緣政治角力也呈現愈演愈烈之勢。

美聯社報導說，此次峰會是有關人工智慧管理規則一系列全球性對話的最新一輪，引人注目的是此輪對話發生在中國原本名不見經傳的深度求索最近突然宣佈通過超低成本硬體開發出的開源人工智慧大語言模型DeepSeek之際舉行。而DeepSeek不僅讓科技界震撼，更有可能推動人工智慧領域進行重大變革。

美國副總統J.D.萬斯（JD Vance）在任內首次出訪，便前往巴黎出席這次人工智慧峰會。中國國家主席習近平則派出中共中央政治局委員、國務院副總理張國清作為特使出席峰會。美聯社指出，這凸顯出美中兩國對此次峰會的高度重視。

美國總統唐納德·特朗普（Donald Trump）表示，他希望通過利用石油和天然氣儲量來滿足能源密集型技術的需求，使美國成為“世界人工智慧之都”。與此同時，他已採取行動撤銷了前總統喬·拜登（Joe Biden）有關人工智慧護欄的行政命令。



報導表示，特朗普正在用自己的人工智慧政策取而代之。該政策旨在通過減少監管壁壘和構建沒有“意識形態偏見”的人工智慧系統來保持美國的全球領導地位。

就中國而言，與2023年人工智慧會議中國只派出一位科技部副部長相比，習近平這次派出一位特使意味著，習近平希望中國在全球人工智慧治理中發揮更大的作用。

DeepSeek上個月的發佈還升級了北京和華盛頓之間圍繞科技霸權更廣泛的地緣政治攤牌。

特朗普表示，DeepSeek為美國科技行業敲響了“警鐘”。而他的人工智慧顧問大衛·薩克斯（David Sacks）則指責DeepSeek使用竊取的OpenAI資料訓練其模型。DeepSeek聊天機器人應用程式現在面臨調查，在某些情況下，由於隱私和安全憂慮，在美國和其他一些國家/地區還面臨禁令。

這次人工智慧峰會由法國和印度聯合主辦，因此法國總統埃馬紐埃爾·馬克龍（Emmanuel Macron）和印度總理納倫德拉·莫迪（Narendra MNodi）將共同主持峰會。

自2022年ChatGPT轟動性地推出後，在英國和韓國舉行的全球AI峰會將世界大國的注意力集中在AI的技術風險上。不過，目前各國控制人工智慧的渴望已經減弱。

“如果我們想要增長、就業和進步，我們必須允許創新者創新、建設者建設和開發人員發展，” OpenAI首席執行官薩姆·奧爾特曼（Sam Altman）在峰會前在法國世界報上發表的一篇專欄文章中說。（VOA）