美拆除80個中共宣傳組織

【看中國記者尹華綜合報導】10月23日，美國國防部長赫格塞斯(Pete Hegseth)宣布，五角大樓已將美國大學校園內由北京資助設立的孔子學院等組織列為國家安全威脅，並在兩個月內系統性拆除了其中80個組織。

時事評論人盛雪認為，此舉並非孤立的教育行政措施，而是特朗普政府對中共展開「全方位、立體化」反共戰略的又一次重要落地。

ALEX WONG/GETTY IMAGES



◀ 10月21日，白宮網絡犯罪會議中，美國總統特朗普聆聽戰爭部長赫格塞斯的發言。

孔子學院的「死灰復燃」

國防部長赫格塞斯在一段影片講話中說，孔子學院是由中共政府支持的「所謂文化中心」，曾滲透到美國幾乎每一個州的大學校園。他說，美國國會幾年前已立法禁止這些孔子學院運作，但它們以不同的形式或名稱繼續出現在校園裏，因此五角大樓決定將其列入威脅美國國家安全的機構名單。

據赫格塞斯介紹，國防部發現，在30所大學裏新出現了80個宣傳組織。這些組織使用不同的名稱和章程，但肩負著同樣的任務，即「竊取知識產權，並滲透美國學生的思想」。他說，國防部在過去兩個月內已經「系統性地拆除了每一個這樣的組織」。赫格塞斯強調：「對任何國家試圖竊取我們辛苦得來的發明，還要讓我們的年輕人反對自己的國家，請記住這個教訓。我們受夠了，再也不會允許了。」

國防部審計完30所大學

就在赫格塞斯發表講話幾天前的10月19日，國防部宣布，已「成功完成」對美國各地30所大學的初步研究安全審計。這些院校均針對其被查出的與《國防授權法》「第1286條清單」受關注實體建立的合作關係採取了緩解的措施，導致80多個合作關係被終止。

國防部說，這些大學所採取的中斷合作行動，有的涉及被納入清單的受關注實體，有的則是「預防性」的，涉及並沒有被明文列入清單的實體。

五角大樓的聲明沒有直接點名中國實體，但列入清單的受關注實體主要位於中國。該清單今年7月公布的最新名單列入130家受關注的外國學術和研究機構，其中88家在中國。

盛雪：不是孤立的教育舉措

盛雪在評論中認為，赫格塞斯的表態不應被視為單純的高校管理問題。她說，長期以來，中共善於利用西方社會的學術自由與開放包容，以語言、歷史、文化教學交流為外衣，將孔子學院打造成意識形態輸出的「橋頭堡」。她稱這是一種「極具侵略性的銳實力滲透」，孔子學院在西方高校內部設立審查機制、干預學術表達，甚至為知識產權竊取和情報蒐集提供掩護。

盛雪指出，特朗普團隊的總體戰略，是要打破過去西方對中共的「綏靖幻想」，從根本上拆解其在自由世界的布局與跨國擴張鏈條。她還總結說，從經貿脫鉤、技術禁運，到能源斷供、打擊毒品與黑產、清除間諜網絡，再到清理意識形態與學術領域的滲透渠道，特朗普團隊正在通過「全維度、深層次的組合拳」，逐步拆解中共在自由世界的滲透布局。她表示，這不僅是捍衛美國國家安全與法治底線，也是在為整個自由世界重塑極權擴張的防線。

國會推擴大清單　中方未應

五角大樓的這些舉措是在國會密切關注下採取的。一直呼籲限制美中科研合作的眾議院中國問題特設委員會主席約翰·穆勒納爾(John Moolenaar)，10月早些時候致函赫格塞斯，呼籲五角大樓擴大「1286清單」，進一步限制中國研究所、實驗室、大學以及人才引進計劃等。

對於五角大樓的最新宣布，中共當局目前尚未做出回應。今年7月五角大樓更新「1286清單」後，中共商務部發言人曾指責美方「不斷泛化國家安全概念」，「將科研合作政治化、武器化、工具化」，並表示中方「將採取必要措施」。

英國呼籲備糧 多國官網下線 人工智能敲響警鐘

【看中國記者路克綜合報導】英國呼籲家庭儲備三天應急物資，多國政府部份網站緊急下線，研究人員更僅花費不到700美元的人工智能調用費用，就發現涉及雲端運算隔離機制的安全漏洞。近期接連曝光的安全事件，讓人工智能對網絡安全的影響，從技術圈推向公眾視野。綜合《金融時報》、美聯社報導及相關機構公告，人工智能正加速發現軟件漏洞，也讓政府和企業面臨更大壓力，必須加快系統排查與安全修補。

英國倡議備糧　風險進家庭

據《金融時報》報導，英國政府10月22日推動「做好準備」宣傳，鼓勵家庭準備足以維持三天的物資，應對自然災害、網絡攻擊或國家支持的破壞活動造成的服務中斷。英國國防大臣施卓添（Wes Streeting）警告，針對關鍵基礎設施的攻擊可能擾亂民眾生活。他強調，公眾需要保持警覺，同時避免恐慌。

這項倡議並非預告全國即將斷糧。英國地方政府說明顯示，應急建議涵蓋停電、斷水、通信中斷和惡劣天氣，相關家庭準備指引自2024年已經存在。儲備耐儲食品、飲用水及照明用品，可以在突發情況下減輕應急部門壓力。當配送、通信和公共服務越來越依賴數碼系統，後台軟件發生故障，影響就可能傳到商店貨架和家庭餐桌。保留幾天生活物資，可以為服務恢復爭取緩衝時間。

政府網站下線　獲修補時間

幾乎同一時間，廣泛用於網站後台的PHP披露兩項嚴重漏洞。10月21日，PHP項目發布安全更新，警告攻擊者在特定條件下可能無需帳號密碼，就能在伺服器上執行代碼。英國國家網絡安全中心建議，各機構盡快識別受影響系統並安裝更新；如果無法及時修補或採取有效緩解措施，應考慮暫時下線。網站關閉，因此可能是主動避險，而非已經失守。10月22日，英國政府在議會確認，32項政府服務無法使用，另外4項部份不可用，主要原因是實施預防性保護措施。當時尚未發現這些漏洞導致中央政府系統遭到確認入侵。

美聯社報導，英國、芬蘭和日本的部份政府網站及服務受到影響。但不能據此斷言，各國政府網絡均已被攻破。這場風波暴露了共同依賴的風險：看似分散的網站，可能運行著相同的底層軟件。一處漏洞被發現，就能迫使不同國家、不同機構同時進入緊急維護狀態。防守方既要搶先完成更新，也要防止倉促修改影響正常服務。

僅用700美元　發現網絡漏洞

安全公司pwn.ai研究人員保洛斯·伊貝洛（Paulos Yibelo）及團隊參與Vercel沙盒安全挑戰，在Linux網絡代碼中發現後來被稱為PwnEscape的漏洞。據團隊技術報告，研究由人類主導，人工智能協助分析源碼、提出假設並驗證結果。

他們在3天內找到關鍵突破口，人工智能介面調用費用不足700美元，隨後在自有實驗環境中演示了從虛擬機突破至宿主機的攻擊鏈。雲端運算的重要前提，是不同用戶的工作負載即使共享物理設備，也應保持隔離。

如果虛擬機中的程序能夠越過邊界，接觸宿主機內存甚至影響其運行，風險就可能超出單個帳號。但700美元未包含專家經驗、人工投入和測試設施；實驗環境中的突破，也不等於商業雲端平台遭到全面入侵。Vercel明確表示，沒有報告顯示客戶數據遭到訪問。值得警惕的是研究效率的變化：複雜漏洞有機會在專家與人工智能協作下更快被發現，同樣的能力也可能被攻擊者利用。

漏洞發現提速　防守時間差

PHP事件呈現了人工智能的雙重作用。研究人員藉助它識別和驗證危險弱點，幫助提前修補；這種能力也可能降低攻擊者研究複雜系統的門檻。

英國政府在議會指出，前沿人工智能有助於發現漏洞，也可能增強網絡威脅。機構需要加快安裝補丁和採取緩解措施，包括依賴外部技術服務商的中小企業。補丁發布只是起點，排查、測試、部署和恢復，仍需要各部門與供應商共同完成。一個迫切問題隨之浮現：當人工智能能在幾天內找到深藏多年的漏洞，人類能否在攻擊發生前完成修補？如果發現速度持續超過修復速度，更多機構是否只能靠暫停服務換取安全？縮短時間差，首先需要政府和企業摸清軟件與供應商清單，明確嚴重漏洞的修復時限，演練斷網、停機後的服務恢復。

雲端平台和人工智能開發商應加強隔離測試、限制智能體權限，防止一次越界演變為大範圍入侵。關鍵開源軟件也需要穩定的維護資金與安全審計支持。人工智能同樣可以幫助篩查代碼、驗證補丁和監測異常，但關鍵系統的修改仍須測試與人工審核。衡量安全能力，不應只看發現多少漏洞，更要看多久完成修復、能否阻止損害，以及系統失靈後，社會還能否維持基本運轉。

WOJTEK RADWANSKI / AFP VIA GETTY IMAGES



▲10月27日，英國國防大臣施卓添在華沙出席記者會。

