

巨龍的新演算法-DeepSeek 對臺灣半導體產業及國安的影響

◎ 許家豪／國立中山大學西灣學院副教授

資料來源：法務部調查局清流雙月刊

先進人工智能（AI）的出現與快速發展，為人類生活帶來極大改變，AI 所衝擊者，不僅是一場技術革命，也是對傳統地緣政治經濟學的挑戰，甚至可能重塑全球權力配置、經濟結構及對於國家安全的重新定義。臺灣作為全球最先進半導體製造、龐大 IC 設計代工、封測產業群集的所在，正處於國際權力競逐的交匯點，而與臺灣有著複雜地緣政治關係的中國，其湧現的強大 AI 模型與平台，更為本已敏感的局面引入了新的變數。

DeepSeek LLM：AI 領域的最新競爭者

2025 年，中國 AI 人工智慧模型 DeepSeek 橫空出世，顯示中國在人工智慧、高效能運算等領域的快速發展，也代表中國積極推動習近平所謂「新質生產力」已有了相當成果。DeepSeek AI 由創辦中國基金「幻方量化」（High-Flyer）的梁文鋒於 2023 年 7 月創立。據該公司說法，其使命是通過解決開發尖端 AI 模型相關的低效率和高成本問題來重新定義 AI，強調資源優化的同時也追求高效能表現。

DeepSeek 在 2025 年 1 月公布其 DeepSeek-R1 大型語言模型（LLM），其有個顯著的特色是對開源（open source）的承諾。DeepSeek 之所以讓人感到驚豔，主要體現在其算法、編碼器、硬體以及系統優化等各方面的創新，也就是透過軟體優化，提高程式碼執行效率，減少資源消耗，從而提高系統整體性能，並能減少硬體資源投入，降低營運成本。實際運用面上，DeepSeek 可以通過差異化競爭來彌補其算力上的不足（相較其他大型的語言模型公司），也可以利用其開源特性，吸引全球的開發者參與到其模型開發和優化中，共同提高其性能和功能，或與其他企業合作，共同開發 AI 應用，實現優勢互補與共同發展。

DeepSeek 的迅速崛起，在受到讚譽的同時也引來多方質疑，特別是其訓練語言資料數據的來源和方法。有指控稱 DeepSeek 可能利用現有 AI 系統（如 OpenAI 等競爭對手）的輸出，來訓練其模型（即所謂的「蒸餾」技術），從而降低訓練成本。這引發了關於知識產權的爭議，以及違反大型模型使用及服務條款的疑義。據報導，微軟觀察到 DeepSeek 相關帳戶從其 AI API 中大量擷取數據，也引發是否盜用商業成果的爭議。

DeepSeek 的雙重限制：國際地緣政治學與中國國內法規

DeepSeek 雖在演算法與模型訓練過程的優化上取得國內外專家的好評，但其

持續發展卻有兩個重大的致命傷。首先是要繼續擴大影響力，必不可少的是硬體設備，但中國高階運算晶片及圖像處理器（GPU）取得不易。眾所周知，美國從拜登總統任內便開始加強對中國半導體產業鏈的封鎖，特別是在減緩中國製造先進製程晶片的能力。這主要體現在：（一）限制如極紫外光（EUV）光刻機等先進製程設備出口，使得中國企業難以獲得生產先進晶片所需的設備。

（二）限制向中國企業轉移包括設計、製造等先進半導體製程及技術。（三）將部分中國半導體企業列入實體制裁清單，限制美國企業與其進行任何商業合作。美國這些封鎖措施確實對中國半導體產業的發展造成了很大的阻礙，使中國在短時間內難以突破技術封鎖，實現自主生產先進晶片。

DeepSeek 在技術報告中自陳其 V3 模型使用的 GPU，是輝達為迴避美國禁令所製的特規 GPU-H800，其算力僅約目前其他 AI 模型的 66%，所以可說 DeepSeek 運算上的創新，其實是因為硬體上的限制所致。但隨著美國不斷加碼限制輝達 GPU 輸出，中國不單無法再購買到 H800，連另一特規降階版本 H20 都已遭川普限制出口。從市占率來看，輝達 GPU 就佔全世界的 90%，而輝達 GPU 所需的核心晶片，也是全球高階晶片市占率佔 90% 的台積電晶片。換言之，輝達與台積電聯手壟斷了全世界的 GPU 供應鏈。

由此，DeepSeek 採取開源模式，而非如同 OpenAI 或其他產品的閉源模式，其實也是種對抗美國技術封鎖的突圍策略，希望藉由中國龐大的中文使用人口和市場，透過大量的資料訓練來替中文 AI 進行特化，另方面則提供國外廠商以 DeepSeek AI 模型為基礎開發的各種運用場景，達成 AI 末端使用者市場的規模經濟與使用市占率，甚或希望在中文 AI 市場發展藉低成本優勢達成應用普及的競爭優勢。這或許是在美國多方圍堵的限制下，中國能提出的最佳解方。

但前開盤算卻可能因中國自身法規限制而產生致命缺陷，因 DeepSeek AI 並不能解決中國獨特的「政治」問題。依中國《國家安全法》以及相關網路安全規定，要求在中國營運的網路應用相關企業必須將數據儲存在中國境內，並同時應遵守「符合中國國情」的言論審查規範。該條限制可理解為，所有投餵給 DeepSeek 的資料、文件或問題，所有權完全屬於中國政府所有，DeepSeek 母公司無權拒絕且必須提供。這將對 DeepSeek 使用者產生嚴重的資安疑慮。所以美國很快作出回應，禁止聯邦或州雇員使用 DeepSeek 服務，雖然 DeepSeek 月費僅為 ChatGPT 的三十分之一，且能透過修改原始碼離線在地使用，做為跳脫母公司伺服器限制的替代方案，但這正是一個低價競爭的陷阱，且相當不利於 DeepSeek 未來商用的獲利能力。

其次，受到中國國安法的限制，DeepSeek 提供的答案必須符合國家法令以及言論標準，這使得 DeepSeek AI 服務的實用性大打折扣。中國的言論審查制度

可能導致數據出現觀點偏差或遺漏，如某些敏感話題可能無法被提及或討論，這會影響數據的真實性和客觀性。其次，企業可能需要修改或刪減數據以符合中國法，導致數據無法反映真實情況。更嚴重者，當生成式 AI 在語料訓練過程，學習越多不實或帶偏見的「資訊」，偏差將越來越嚴重，甚至產生數據污染或 AI 幻覺 (AI hallucination)。事實上，言論審查與開源模式兩者間存在難以化解的衝突。數據過濾及言論審查機制可能會對開源社群的數據收集和共享產生影響，包含敏感信息的數據無法被收集或公開，將影響到模型的訓練效果。

臺灣的半導體霸權與國家安全要務

臺灣製造了全球約 65% 的半導體及超過 90% 的高階晶片，另在 IC 設計領域，臺灣擁有僅次於美國的全球第二大市占率，使得世界產生對臺灣半導體的依賴，也常被稱為「矽盾」。半導體產業鏈不但是臺灣經濟繁榮的基石，也是國際安全戰略布局的重要因素。然而，也因地緣政治因素，臺灣持續面對來自中國的嚴峻國家安全挑戰，體現在軍事威懾、灰色襲擾、經濟脅迫以及分化臺灣社會與治理的複雜假訊息攻勢。因此，DeepSeek AI 模型的出現也為臺灣的國防規劃和韌性建設增添了另一層複雜性。例如臺灣政府部門或民間公司使用 DeepSeek AI 服務進行敏感的研發或設計工作，考慮到依中國法規，所有數據都須回傳中國進行運算，可能立刻面臨知識產權洩露或產業間諜活動的風險。即便使用開源模型，也需要仔細審查，以確保它們不包含後門或數據竊取機制。

作為原生的中文生成式語言模型，DeepSeek 可能帶來的國安威脅，除了政府與民間機密外流以及民眾過度依賴產生的戰略脆弱性之外，更大的威脅其實是 DeepSeek 能成為訊息戰與認知戰的極有效工具。民眾可能在使用 DeepSeek 時，誤認 AI 工具都如實作答，而未意識到 DeepSeek 的回答其實是建立在中國言論審查機制之上，從而產生「習得性偏差」(learned bias)，亦即 DeepSeek 其實本身即帶有統戰效果。再者，不少研究報告指出，中國利用 AI 生成和散播旨在製造臺灣內部分裂的假訊息。透過 DeepSeek V3.1 這種語言模型，能輕易在短時間內產生大量社群軟體假帳號、自動生成大量類似回覆、甚至與真實網民對談吵架。這種透過生成式 AI 模型進行網路攻擊與認知戰，早已超越吾人的認知，更加複雜、個人化、範圍更大且全天候的攻擊模式，更難被偵測和反制。

新一代 AI 編碼器亦可用在開發更強效的惡意軟體或工具，快速識別網路漏洞並進行自動化攻擊，進而危及臺灣的關鍵基礎設施。當然，臺灣並非被動的觀察者，政府和產業界正在探索以 AI 進行防禦，包括 AI 驅動的網路安全系統、反制假訊息的情報分析工具等，都顯示政府部門對安全威脅的警覺。

結論：半導體、AI 與地緣政治

DeepSeek 的出現，使 AI 發展、半導體領導地位及全球地緣政治之間日益加深的糾葛具體化，而臺灣正處於此風暴的中心。

「矽盾」理論取決於臺灣在先進晶片製造方面的近乎壟斷地位。如果臺灣能有效整合 AI 進一步增加技術更新與產能，將可以進一步擴大其在半導體領域的技術領先地位，則至少在中期內可以強化此盾牌。然而矽盾若越成功，意味著美國對臺灣的依賴加深，使其必須承受戰略上的脆弱性，因此美國一方面將必須透過軍力嚇阻中國輕率發動臺海戰爭，但另一方面卻必須用政策手段說服台積電在美、日、德設廠，對臺灣來說反而是弱化矽盾的效力。

中國先進 AI 的崛起，意味著臺灣必須採取一套全面且多管齊下的戰略，不僅包括鞏固臺灣在半導體領域的技術優勢，還包括發展一個強健的本土 AI 生態系統作為國家戰略目標，打造專注於創新以及合乎 AI 倫理、且較不具資安風險的模型。這也意味著深化與民主夥伴在供應鏈韌性、AI 治理和國防技術方面的合作。

具體的政策建議包括：（一）培育本土 AI 人才與創新：投資於教育、研究和基礎設施，以在臺灣內部建立一個世界級的 AI 生態系統，並根據其獨特優勢和需求進行調整；（二）強化網路安全與知識產權保護：為關鍵基礎設施和半導體產業建立強大的防禦機制，以應對 AI 驅動的攻擊和間諜活動，並配合嚴格的知識產權保護措施；（三）深化國際合作：與可信的民主夥伴在 AI 研究、倫理準則、供應鏈安全和情報共享方面密切合作，以應對共同威脅；（四）審慎評估與風險管理：仔細評估採用任何 AI 工具（尤其是那些與我國具有地緣政治利益衝突的國家）的效益和風險，並為其使用建立明確的規範；（五）增強社會韌性：教育公眾認識 AI 驅動的假訊息，並提升媒體素養以反制認知戰；（六）持續關注地緣政治環境：正視 AI 及半導體供應鏈並非只牽涉到科技技術的創新，更是牽動全球地緣政治變遷的重要因素，在擬定 AI 相關產業人材政策時，同時必須培養地緣政治學以及半導體國際政治經濟學的專門人才。