

議題研析

一、題目：美國「人工智慧緊急停止機制法案」(AI Kill Switch Act)簡析

二、議題所涉法規

人工智慧基本法

三、背景說明（緣起）

報載美國生成式 AI 業者於進行新一代模型測試及開發過程中，發生 AI 模型突破測試環境隔離機制，並對外部網路服務進行未經授權操作等情形。此外，部分高階 AI 型因具備較高程度之網路操作及潛在攻擊能力，亦衍生資訊安全與國家安全等疑慮。為因應前述事件所凸顯之 AI 模型於部署後可能發生失控，或因安全防護機制不足而產生之潛在風險，美國國會跨黨派議員共同提出「人工智慧緊急停止機制法案」，要求最先進 AI 系統之開發業者具備降低模型運作能力、暫停服務及全面停止系統運作等技術能力，引發對於高風險 AI 系統之監管機制、業者責任及政府介入權限等法制議題之相關討論¹，值得關注。

四、問題爭點

為降低 AI 模型失控引發網路攻擊所可能衍生之風險，美國跨黨派國會議員近日提出「人工智慧緊急停止機制法案」，賦予政府於判斷 AI 模型可能造成危害時，強制停止或關閉該模型之權力。對此，科技業界已就過度監管可能限縮 AI 發展之多元性表達疑慮，並主張

¹ Ted Lieu, Reps Lieu and Moran Introduce Bill to Require Kill Switch for AI Systems That can Cause Catastrophic Harm, 115 年 8 月 26 日，網址：<https://lieu.house.gov/media-center/press-releases/rep-lieu-and-moran-introduce-bill-require-kill-switch-ai-systems-can>，最後瀏覽日期：115 年 8 月 26 日。

政策制定者應審慎避免對開放模型施加過度限制，以兼顧 AI 安全與技術創新、市場競爭之發展²。本文謹簡析相關內容，供本院委員問政及修法參考。

五、探討研析

（一）美國「人工智慧緊急停止機制法案」簡介

為回應近期 AI 系統於測試期間發生失控並發動網路攻擊之事件，美國國會跨黨派議員於 2026 年³7 月 23 日聯合提出「人工智慧緊急停止機制法案」，要求 AI 系統開發業者具備足夠之技術能力，對其所研發之 AI 系統採取限制、暫停或關閉等措施，以確保 AI 系統失控所衍生之風險維持於可控範圍內。該法案亦賦予美國國土安全部、商務部及國家情報局命令停止或限制使用可能造成重大損害之 AI 系統之權限。依美國智庫調查，約有 86% 之跨黨派選民支持本法案所要求 AI 開發業者對瀕臨失控之 AI 系統須具備相應之控制及停止能力，以避免 AI 工具因失控而造成難以挽回之損害⁴。

本法案之規範重點，除規定 AI 系統開發業者對其所研發之系統須具備足夠之風險控制能力外，亦強調分級應變機制（graduated response framework）之建立，使主管機關得依 AI 系統事故之嚴重程度採取系統降速至完全停止運作等不同之應變措施；此外，本法案亦要求業者建立事故報告機制，並妥善保存相關事件之調查記錄，以利後續檢討修正相關措施⁵。有關罰則部分，業者倘違反本法案相關規定，將面臨最高 200 萬美元之罰鍰⁶。

（二）美國科技業者聯名致函國會表達擔憂之立場

為表達對「人工智慧緊急停止機制法案」可能威脅科技創新發展之擔憂，近 30 家美國科技大廠於 2026 年 7 月 24 日以「開放權重與美

² 本公開信函係由美國 25 家科技企業及組織所共同發布。Open Weights and American AI Leadership, 2026 年 7 月 24 日，網址：<https://images.nvidia.com/pdf/Open-Weights-and-American-AI-Leadership.pdf>，最後瀏覽日期：115 年 8 月 27 日。

³ 本文有關年分之使用，原則以民國紀年表述，惟涉及外國參考資料部分，改採西元紀年表述。

⁴ Ted Lieu，同註 1。

⁵ Ted Lieu，同註 1。

⁶ Rep. Lieu, Ted, H.R.9917 - AI Kill Switch Act, 2026 年 7 月 23 日，網址：<https://www.congress.gov/bill/119th-congress/house-bill/9917/text>，最後瀏覽日期：115 年 8 月 27 日。

國 AI 領導力」(Open Weights and American AI Leadership)為題，聯名致函美國國會，表達支持開放權重 AI 模型之發展及應用，並呼籲立法者應避免對開放權重 AI 模型增加過多限制而抑制產業發展之立場⁷。

聯名信函中強調，衡量美國 AI 領導力的標準端視美國能否建立一個強大、開放並能導入到各產業的放權重 AI 生態系。信函中亦正視開放權重 AI 模型的危險性，並呼籲政府應採適當方式管理此類風險而非以強硬手段禁止其應用。在現今網路攻擊事件大量運用 AI 技術之情況下，資安人員須具備足夠先進之模型，始能有效偵測、模擬並因應推陳出新的網路威脅，開放權重 AI 模型可以擴大資安防禦能力、提升透明度，使不同技術團隊得以共同發掘並修補系統漏洞，成為確保 AI 安全與資安防護之重要工具。立法者對於此類模型之發展若施加過多限制措施，不僅有加劇相關風險之虞，亦可能削弱 AI 產業之市場競爭力⁸。

(三) 結語

在 AI 技術快速發展的時代下，現行法規之訂修往往難以即時回應新興科技所衍生之法律風險及治理需求，惟若採取貿然激進的限制措施亦可能面對扼殺創新、削弱國家發展競爭力之隱憂。美國「人工智慧緊急停止機制法案」係為回應 AI 系統失控發動並可能網路攻擊之風險所提出之法案，旨在透過要求業者建立嚴格的風險控管機制降低 AI 技術遭濫用或失控所造成之負面影響。然而，相關措施卻引發業界對於過度監管，將對 AI 創新發展形成阻礙，進而影響國家競爭力之疑慮。

面對新興 AI 模型於訓練、開發及實際應用過程中因失控所衍生之網路風險，立法者應如何於健全產業創新發展環境及人民權益保障間取得平衡，並非易事。近期美國對於本法案之產業對話及監管討論，值得我國持續關注，以確保未來能在兼顧科技創新與產業發展下，建立更具彈性且符合科技發展趨勢之監管架構。

撰稿人：陳樂庭

⁷ Open Weights and American AI Leadership，同註 2。

⁸ Open Weights and American AI Leadership，同註 2。