各國發展主權AI策略對我國的啟示

⊙廖明輝／中華經濟研究院第二（國際經濟）研究所　計畫輔佐研究員
⊙洪尉淳／中華經濟研究院第二（國際經濟）研究所　分析師

各國發展主權AI策略在於確保人工智慧技術自主性，減少對外國技術依賴，並維護國家經濟和安全利益。臺灣發展主權AI需採取「以應用為中心」的戰略，強化數位基礎設施和AI人才培養，讓產業能夠做到應用自主化；並將AI產業化，擴大AI在產業及社會的應用。如此，臺灣才能在全球AI競逐保持競爭力，確保數位主權，進而維護國家安全和經濟利益不會受到外部依賴所影響。

關鍵詞：主權人工智慧、生成式人工智慧、世界經濟論壇
Keywords: Sovereign AI, Generative AI, World Economic Forum

主權AI對主權國家的重要性

世界經濟論壇（World Economic Forum, WEF）於 2024 年 4 月發布「發展主權 AI 的六大戰略支柱」[1]，指導各國在考量經濟成長與國家安全前提之下如何發展主權 AI（Sovereign AI）。WEF 將主權 AI 定義為「國家透過規劃及建立自己的人工智慧基礎設施、核心能力和產業，以增強國家競爭力並維護未來發展」。此外，輝達（Nvidia）也提出主權 AI 的觀點，認為「主權 AI 是指一個國家利用自己的基礎設施、數據、人才和商業網絡，產出本國的人工智慧能力」[2]。因此，主權 AI 意指國家需要掌控自己的 AI 系統和相關數據，避免對外國技術的依賴，從而減少他國對自己國家經濟、文化和社會發展的控制或影響。

主權 AI 包括一個國家開發符合其核心價值人工智慧的企圖心和能力，進而維護國家數位主權和安全。它的出現是由於各國在人工智慧領域的不信任感日益增強以及科技公司的主導地位。作為一項戰略資產，國家必須了解主權 AI 的重要性，因為它可以增強經濟和社會發展、創新、生產力和國家安全。尤其隨著生成式 AI（Generative AI）興起，顯著的創新潛力也伴隨風險，如失業、

錯誤與虛假訊息和深偽造假等，對社會、經濟和國家安全構成嚴重挑戰。WEF 即指出，主權 AI 在經濟和國家安全層面上具有重要的意義。從經濟層面而言，透過自主開發和應用 AI 技術，國家可以在醫療、金融、交通等關鍵領域提升效率和創新能力。此外，建立本土的 AI 產業還可以促進高科技產業發展，從而帶動其他相關產業鏈的成長，形成國家競爭優勢。在國家安全方面，主權 AI 可以透過開發和應用 AI 技術增強國防能力。而且主權 AI 能幫助國家掌控關鍵數據和技術，減少對外國技術的依賴，讓國家能夠免於各種「脫鉤斷鏈」的影響。此外，AI 是一種規範性技術，深刻影響國家社會在創造和利用 AI 的價值觀、權利和原則。因此，各國需要有能力根據其獨特的願景來塑造和管理 AI，確保服務於其國家利益。

以生成式 AI 的發展來說，其迅速崛起預計將在未來十年內使全球 GDP 成長百分之七。然而，這些利潤主要由少數私人企業掌控，對於政府而言，完全依賴外部供應商將對國家安全和經濟競爭力構成風險。因此，國家需要建立主權 AI 模型，如英國提倡建構「Chat-GB」，創建獨立的技術架構來支持公共服務如國民醫療服務體系（NHS）和政府、國防情報等，否則就會面臨過度依賴美國 Google Bard 及 OpenAI ChatGPT 的風險。主權 AI 允許各國了解其模型的訓練過程及所用數據，從而在模型中灌輸本國價值觀。尤其對於英語主導的人工智慧模型而言，其背後的文化刻板印象往往偏向美國。臺灣在中文語言模型也面臨與英國同樣的處境與挑戰，目前中文訓練的數據主要來自中國大陸，往往隱含中共的價值觀與政治主張，年深日久將對臺灣影響深遠。因此，發展主權 AI 將可以選擇本國的語言和文化資源進行訓練，以確保語言模型的生成輸出能夠更加適應本國需求。

實現主權AI的關鍵與挑戰

實現主權 AI 的關鍵在於本土人工智慧的發展，也就是一個國家不依賴外部資源的創新能力，使人工智慧發展和治理與國家價值觀能保持一致。前述提及的主權 AI 包含兩個面向：國家企圖心和獨立系統。在國家企圖心面向上，主權 AI 意指各國如何策略性地培育自己的人工智慧能力，客製化人工智慧開發以應對特定的國內挑戰和需求。例如，有些國家可能會專注於醫療保健領域的人工智慧，以滿足人口老化的需求，有些國家則優先考慮農業領域的人工智慧，以加強糧食安全。另外，主權 AI 也涉及一國減少對國外開發之人工智慧解決方案的依賴，目的是防範漏洞並確保對關鍵技術的控制，特別是具有軍事或經濟影響的技術。此外，各國更強調透過對研究、教育和技術人力發展的投資，促進國內創新並培養人工智慧相關領域的人才。

除了國家層面之外，主權 AI 還涉及人工智慧系統本身的技術能力層面。這些系統應該要具有以下特點：他們能夠獨立工作，不需要外部基礎設施或由他人控制的服務。不

僅增強安全性，還透過減少潛在漏洞來保護資料隱私。這些系統利用其本身範圍內儲存和管理的資料進行訓練，避免對可能帶來偏見或隱私風險之外部資料集的需要。它們是針對特定任務量身訂製，有助於簡化複雜性、並減少產生與過於廣泛功能相關之漏洞的可能性。雖然這些自給自足的系統可以提供增強的安全性和資料隱私等優勢，但它們也有其缺點，它們的專業性可能會限制適應性，並減緩通用人工智慧的進步。

不過，實施主權 AI 有其自身的一系列技術挑戰，例如數據稀少和偏差，這些系統可依賴的國家數據庫可能有其規模限制，數據來源也可能有固有潛在偏差。另外，訓練大型模型需要大量的運算能力和基礎設施，可能超出國家能力。再者，建構和維護此類系統需要深厚的人工智慧專業知識，而某些國家可能缺乏這些專業知識，無法建構能夠確保免受網路攻擊和保護訓練資料安全所需要的強大解決方案。

各國發展主權AI策略

如前所述，WEF 已經定義主權 AI 係指各國根據當地政策或國家人工智慧戰略，利用本土人才建構人工智慧的能力。建設這種能力有助強化國家保持經濟競爭力和維護自身價值觀，並且支持國家在航空航太、國防、教育、住房、交通、公共安全、供應鏈和製造業等各個領域的利益。在發展策略上，WEF 於 2024 年 4 月所發布「發展主權 AI 的六大戰略支柱」，指導各國在經濟成長與國家安全的前提下，透過多方面的策略支持以發展和實現主權 AI。六大戰略支柱的政策內容請見表 1。

值得注意的是「人才」的重要性，WEF 認為「人工智慧發展需要依賴大量訓練有素的本土人才，而不僅僅依靠政策推動」[3]。而且只有本土人才才能確保國家各產業領域的人工智慧應用，能夠切合國家社會實際需求。據此，WEF 進一步在 2024 年 7 月發布《國家如何建立主權 AI 和本土人才以提高經濟競爭力》報告，為全球各國提供建立主權 AI 的具體指引。其中即提到政府的資源投入應該集中在提升人工智慧人才的培養和引進，才是創造競爭優勢的關鍵。各國政府必須認知到，人工智慧的發展需要在地化生態系統的支持，包括在地人才、在地問題、在地資本、在地研究、在地中小型企業、在地大學和科技大學等。據此，「人才」成為評估國家發展 AI 程度的重要關鍵之一。

進一步觀察近期全球各國在 AI 領域發展程度的狀況。根據英國 Tortoise Media 公布的 2023 年「全球人工智慧指數」[4]，從人才、基礎設施、營運環境、研究、發展、政府策略、和商業等七個維度進行評估。2023 年排名前五名的國家分別是美國、中國大陸、新加坡、英國和加拿大（如表 2）。這些國家在基礎設施、營運環境、研究、發展、政府策略和商業應用等方面均有突出表現，而這些維度的提升都須要靠人才的支撐。

表1　發展主權AI的六大戰略支柱

發展主權AI戰略	內容
數位基礎設施	各國應建立配備先進運算能力的資料中心，有效處理和分析大量數據。落實資料在地化政策以確保數據安全並增強數據主權，為人工智慧技術的開發和部署提供穩固基礎。不僅保障數據的安全性和隱私性，也能確保國家面臨外部技術封鎖時，仍能自主運作和發展
勞動力發展	勞動力發展是人工智慧技術進步的基礎。各國應推動STEM教育，更新教育課程納入人工智慧和機器學習內容，並提供職業培訓計畫和終身學習機會，確保擁有推動國家人工智慧產業發展的人才儲備。熟練的人才是人工智慧創新和應用的關鍵，各國需不斷提升本土人才的知識和技能，滿足產業發展需求
研究、開發與創新	研究、開發與創新是推動人工智慧技術突破的動力來源。政府應提供資金和激勵措施，支持基礎和應用研究，並促進創新的商業化。建立共生的創新生態系統，促進產業參與者、學術機構和研究機構之間的合作，推動技術突破和國家競爭力的提升
監管和道德框架	制定全面監管和道德框架，針對隱私、透明度、數據保護和網路安全等問題，制定明確指導方針和監督機制，確保人工智慧技術的負責任使用。不僅有助提升技術的信任度，還能防範技術濫用和風險，保護社會公共利益
激勵人工智慧產業	激勵人工智慧產業是推動經濟成長的重要手段。各國應創造有利的環境，推動人工智慧驅動的業務和應用發展，尤其是在能源、醫療保健、金融、交通和製造等關鍵領域。政府應提供稅收減免、補助金和簡化專利流程等激勵措施，促進創新創業，並鼓勵公共部門率先採用人工智慧技術
國際合作	雖然主權人工智慧強調本土能力建設，但國際合作有助於制定全球人工智慧標準，共同應對隱私和網路安全威脅。國際專案合作可以匯集資源和專業知識，加速技術進步，實現互利共贏。全球範圍內的合作可以促進技術交流和知識共享，共同應對人工智慧帶來的挑戰

資料來源：作者整理，部分內容取自 World Economic Forum (2024). Emerging Technologies-Sovereign AI: What it is, and 6 strategic pillars for achieving it. https://www.weforum.org/agenda/2024/04/sovereign-ai-what-is-ways-states-building/

表2　2023年全球人工智慧指數排名前五名國家

國家	排名	執行面（Implement）			創新面（Innovation）		投資面（Investment）	
		人才	基礎設施	營運環境	研究	開發	政府策略	商業
美國	1	1	1	28	1	1	8	1
中國大陸	2	20	2	3	2	2	3	2
新加坡	3	4	3	22	3	5	16	4
英國	4	5	24	40	5	8	10	5
加拿大	5	6	23	8	7	11	5	7

資料來源：Tortoise (2023). The Global Artificial Intelligence Index.

不論是全球主要 AI 參與者包括歐盟、中國大陸、美國，或是其他 AI 發展緊跟在後的國家如印度、新加坡與荷蘭等，每個國家都有不同的願景和優先事項，影響其在追求主權 AI 的相關做法。例如，歐盟的目標是打造值得信賴、以人為本的人工智慧，專注於提高技術能力、確保健全的道德框架以及加強歐盟內部和全球範圍內的合作。

相較之下，中國大陸將人工智慧視為戰略重點和國家目標，展現其加速發展、廣泛應用和有效治理的雄心。中國大陸的戰略重點是開發、應用和治理，目標在充分利用人工智慧的潛力來推動經濟成長、增強國家安全並增強其全球競爭力。

美國則將人工智慧視為創新和領導力的源泉，專注於增加研究經費、促進人工智慧技術的廣泛採用以及實施平衡創新與監督的監管框架，旨在保持其在人工智慧開發領域的領導者地位。

英國的策略則聚焦於研究、開發和部署，透過優先投資卓越研究、培育人工智慧產業的發展以及建立全面的治理框架來實現人工智慧能符合道德和負責任的使用。

印度的「印度 AI 使命」（India AI Mission）計畫投資 12.5 億美元開發運算基礎設施和大型語言模型，建造配備至少一萬顆 GPU 的超級電腦以建立強大的 AI 運算基礎設施。

新加坡則與輝達合作，建立「東南亞語言同一網路」（SEA-LION）大型語言模型，透過訓練東南亞十一種地區語言的資料集以適應東南亞的多元語言環境並支持新加坡的「國家 AI 策略 2.0」。

荷蘭政府則積極發展開放式大型語言模型 GTP-NL，促進符合荷蘭的公共價值觀並尋求歐盟投資超級電腦，共同推行歐洲主權 AI 計畫。透過價值驅動方式，荷蘭企圖在 AI 領域成為歐洲領導者，並透過歐洲成為世界的領導者[5]。

臺灣發展主權AI的策略

我國也注意到當前「主權 AI」的發展趨勢。國科會主委吳誠文於今（2024）年 6 月即表示，為因應主權 AI 興起，臺灣將推動「關鍵應用系統國產化」。他強調臺灣擁有領先世界的半導體技術，應積極發展自己的應用系統以鞏固資安與國安。臺灣若能明確定義應用需求，市場將隨之浮現，產業也將抓住機會投資發展。因此，要強化主權 AI，臺灣必須建立自主 AI 系統，讓產業在未來能夠做到應用自主化；也能讓關鍵技術留在臺灣，以避免供應鏈斷鏈風險[6]。

在此觀點下，本文認為面對當前迫切的重大挑戰，如氣候變遷、能源需求增加、少子化與人口老化、以及中國大陸對臺灣民主自由和安全的威脅，我國發展主權 AI 或應採取「以應用為中心」的戰略：基於「關鍵應用系統國產化」概念建立必要的生態系，強化既有 AI 研究開發能量與基礎建設，協助相關 AI 產業發展，培育各產業所需 AI 人才，進而持續促進「產業 AI 化、AI 產業化」，擴

大 AI 在產業及社會的應用。

進一步而言，我國發展主權 AI 的具體作法，或可從以下幾點著手。首先，需要建立更強大的數位基礎建設，除了必要通訊建設外，持續強化發展超級電腦也很重要。目前我國除了國網中心的「臺灣杉」二到三號及創進一號外，也與輝達合作建置「Taipei-1」超級電腦，我國應持續投資建置具備更強大算力的 AI 超級電腦以加速 AI 研究。對於資料部分也必須確保資料主權和安全性。

第二，在研究發展與創新方面，我國應強化關注與「產業應用」有關的研發創新，促進「產業 AI 化」，協助產業導入具體 AI 應用場景的商業模式；同時政府應該提供激勵措施培育在地 AI 產業，鏈結各項產業應用，達到「AI 產業化」。此外，我國目前已有由國科會發展具有臺灣特色與繁體中文的可信任生成式 AI 對話引擎「TAIDE」（Trustworthy AI Dialogue Engine），應該擴大推動百工百業鏈結 TAIDE 投入更多應用，也才能持續精進此一我國自行開發的重要大語言模型。另外，政府本身也可以在 AI 應用上扮演重要角色，在「公共服務」導入 AI 運用，參考新加坡政府開發減輕公務人員負擔的「Pair」專案以導入生成式 AI，在保障資料安全的前提下大膽實驗新科技。

第三，臺灣應致力培養各類型 AI 應用系統的研發人員，確保數位人才能夠跟上 AI 技術的快速進展。第四，AI 相關的監管和道德框架也是確保我國主權 AI 發展的關鍵，今（2024）年底將提出的《AI 基本法》草案，需明確訂定保障人權與人類自主的原則，確保 AI 技術被負責任地使用，以人為中心並保留人類決策權。

最後，臺灣應該積極參與國際對話與合作，建立標準並共同應對隱私和網路安全威脅。如此，臺灣才能在全球 AI 競賽中保持競爭力，確保數位主權，進而維護國家安全和經濟利益不會受到外部依賴所影響。

附注

1. World Economic Forum (2024). Emerging Technologies -Sovereign AI: What it is, and 6 strategic pillars for achieving it. https://www.weforum.org/agenda/2024/04/sovereign-ai-what-is-ways-states-building/
2. NVIDIA (2024). What Is Sovereign AI. https://blogs.nvidia.com/blog/what-is-sovereign-ai/
3. World Economic Forum (2024). Emerging Technologies - How nations can build sovereign AI and homegrown talent for economic competitiveness. https://www.weforum.org/agenda/2024/07/sovereign-ai-talent-improve-economic-competitiveness/
4. Tortoise (2023). The Global Artificial Intelligence Index. https://www.tortoisemedia.com/intelligence/global-ai/#rankings
5. 自由時報（2024）。主權AI崛起 臺灣面臨保衛戰。https://talk.ltn.com.tw/article/paper/1637862
6. 工商時報（2024）。主權AI興起 吳誠文 推應用系統國產化。https://www.ctee.com.tw/news/20240625700049-439901