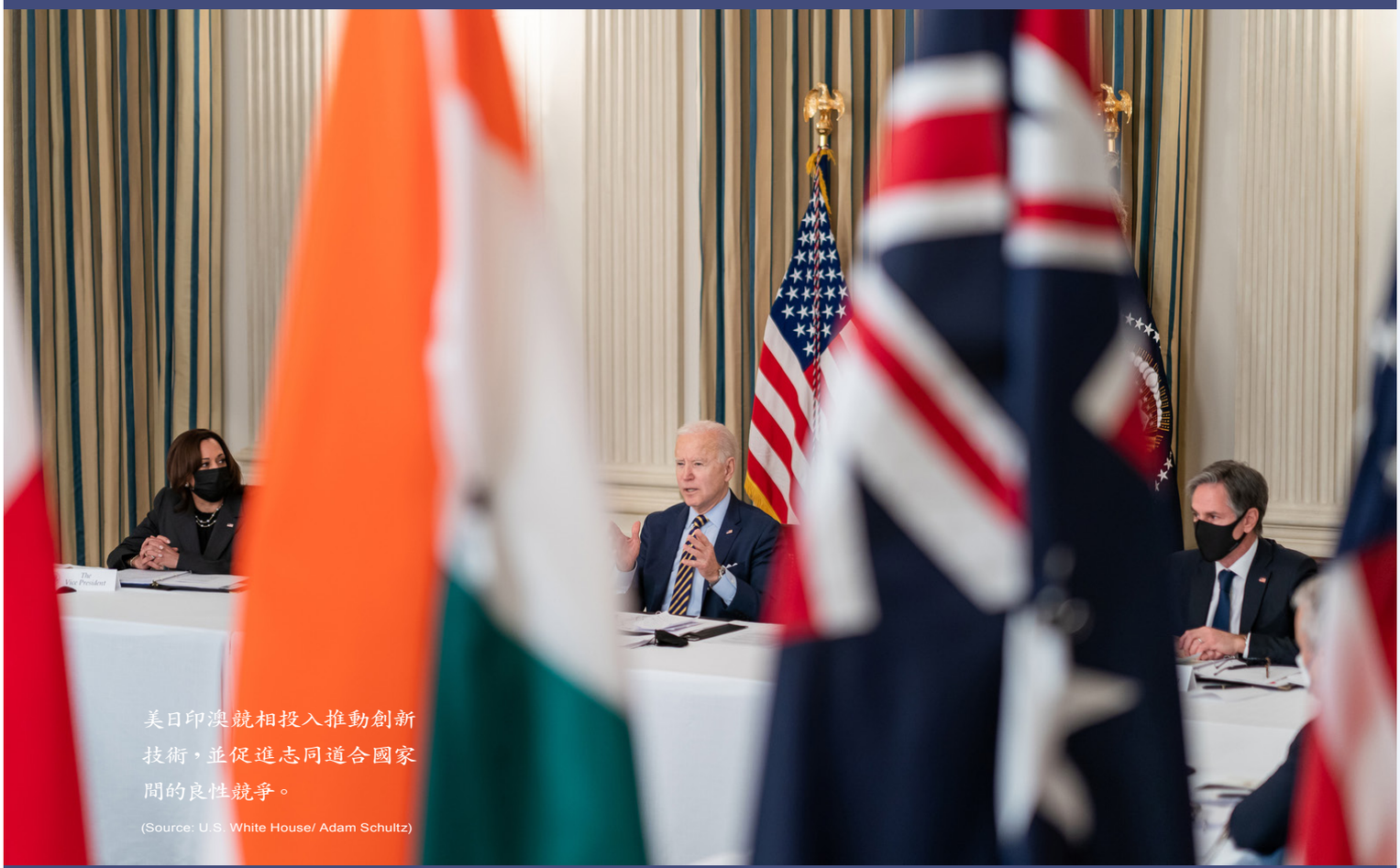
作者/Abhijnan Rej　譯者/劉慶順　審者/馬浩翔

2030印太人工智慧發展

Artificial Intelligence for the Indo-Pacific: A Blueprint for 2030

取材/2020年11月27日外交家網站專文(*The Diplomat*, November 27/ 2020)

當全球技術競爭加劇時，地理範圍涵蓋印度洋與太平洋的「印太」戰略架構已然出現；該架構的主要倡導者包括澳大利亞、印度、日本以及美國。這些國家指出，印太地區必須是自由、開放、具韌性以及包容的。



美日印澳競相投入推動創新技術，並促進志同道合國家間的良性競爭。

(Source: U.S. White House/ Adam Schultz)

即便是最漫不經心的當代國際政治觀察家，也能證明（雖不盡然如此）主要發生在美國及其盟邦與中共及俄羅斯間的技術競爭又再次出現。迄今，分析人員已從各種角度研究此議題：對軍事平衡的意義、國際合作的可能性，以及技術優勢對國內政策的意涵等。川普政權將與中共間的技術競爭，視為其戰略性政策的基石，並強調美國必須在包括「人工智慧」(Artificial Intelligence, AI)、「量子資訊科學」(Quantum Information Science)、航太及其他關鍵技術等各方面保持優勢。

諸如澳大利亞、印度以及日本等其他「印度洋—太平洋」(Indo-Pacific，以下簡稱印太)地區的國家，也競相投入在國內推動新式與新興技術，並且促進「志同道合國家」間技術合作之競爭。2020年6月，有14個國家與歐盟共同啟動了「全球人工智慧夥伴關係」(Global Partnership on Artificial Intelligence)，以促進人工智慧的集體研究與實現。澳大利亞與印度致力針對包括人工智慧在內的一系列關鍵技術進行合作，而美國國防部則尋求與盟邦及夥伴國，就人工智慧相關技術與實際應用進行合作。另美國智庫也發表了探尋在人工智慧及建立「聯盟創新基地」方面更多國際合作之可能性的報告。

人工智慧合作：內容與緣由

在技術競爭加劇的同時，地理範圍涵蓋印度洋與太平洋的「印太」戰略架構已然湧現；該架構的主要倡議者和關心新式與新興技術在決定未來地緣政治平衡中所扮演角色的，是同一批國家，包括澳大利亞、印度、日本以及美國等。這些國家指出，印太地區必須「自由」、「開放」、「具韌性」且「包容」。就實務上而言，這些形容詞意指印太地區免於中共在經濟或任何方面的威脅，亦即不允許出現與「全球公域原則」(Global-commons Principles)背道而馳的「專屬領土主張」(Exclusive Territorial Claims)，且能在衝擊中具韌性(特別是這點在新冠肺炎肆虐期間已獲得證實)。此外，該地區亦必須能夠「包容」，這意味印太地區的願景必須涵蓋所有區域國家的需求與觀點。對中共之「灰色地帶威嚇」(Grey-zone Coercion)與「混合戰」(Hybrid Warfare)及其「區域基礎設施外交」(Regional Infrastructure Diplomacy)的關注，已加劇了許多印太地區行為者對該地區軍事力量平衡局面轉變為倒向中共的憂慮。

在接下來的內容中，筆者將探討圍繞著可促進區域合作的三項人工智慧技術，這些技術可在2030年中期前，進一步協助促進印太地區的自由、開放、更具韌性以及包容性。會如此討論係假設現行技術趨勢將在未來十年持續，且該地區所面臨的挑戰與機會也將與今日無異。就其戰略用途而言，筆者認為：

「空間計算技術」(Spatial Computing Technology)係維持該地區開放的手段，而該技術充分利用「地理空間資訊」(Geospatial Information)的能力，則可用來強化傳統軍事戰力；具韌性的智慧基礎設施係重新激發區域吸收對社會技術與實體基礎設施之衝擊能力的手段；「反敵對技術」(Counter-Adversarial Technologies)則可協助區域國家對抗假資訊以及新興網路攻擊，使其得

以抵抗非動能武器威脅，藉此維持區域之自由特性。然而這三種技術都具備廣泛的商業與公共福利用途，這促使筆者接下來探討此議題具包容性的面向：選擇這些技術的用意，或多或少是為了鼓勵那些不想捲入「中」美競賽漩渦，而傾向以更具建設性的技術合作議題來解決其特殊情況的國家來參與國際人工智慧合作。

空間計算技術

籠統來說，空間計算係指能強化人類與其地緣環境互動能力的各種計算技術。如電腦科學家謝卡爾(Shashi Shekhar)在其於2019年出版的合著書中指出，「空間計算乃是藉由理解現實世界、認識並傳達吾人與世界之關係，並且行經這些地點，以轉變吾人生活的一套理念與技術」。吾人相當熟悉「全球定位系統」，乃至於「遙控感測」(Remote Sensing)及「地理資訊系統」(Geographical Information Systems)等空間計算，但這只是開端。空間計算的熱烈鼓吹者展望能在不久的未來看見蘊藏在「空間預測分析」(Spatial Predictive Analytics，即檢測地理與空間資料中之有用模式的技術)、「位置感知物聯網」(Location-aware Internet of Everything；可將活動物體連接至固定智慧目標)，以及無縫整合來自室外、室內、水下與地下地理環境資料等的可能性。

然而，在空間計算所能提供的各項可能性中，又以「擴增實境系統」(Augmented Reality Systems)最為引人注目。如同三位擴增實境議題專家所定義，「擴增實境可透過即時覆蓋空間調整影像的技術，豐富吾人對現實世界的感知。」除在軍事應用外，擴增實境在商業應用方面的可能性也是眾所周知；2016年運用該技術的手機遊戲「精靈寶可夢GO」(Pokémon Go)即是證明。

科技權威凱利(Kevin Kelly)從擴增實境觀察到「鏡像世界」(Mirror World)中令人振奮的可能性。如同他於2019年2月在《連線》(Wired)月刊中所發表的那篇頗具影響力的文章所指出般：「很快地，總有一天現實世界中的每個地方與事物(每條街道、燈柱、建築物還有房間)都將在鏡像世界中擁有與原物般大小的「數位孿生」(Digital Twin)。」有鑑於印太地區國家資助之駭客如此頑強與機會主義當道，假如此類情況終將肇生，所形成的安全挑戰將顯而易見。凱利接著補充道：「連接到網際網路的事物，都將會連到鏡像世界」。此外，假使現行之物聯網預測以及凱利的自信預言(在2030年將會有500億臺設施透過龐大網絡連接)都成真，那麼擴增實境將極有可能同時帶來全新契機與威脅。

人工智慧與空間計算間的關係密不可分。在地理區域中感測器與效應器數量增加後，其所蒐集到與空間環境有關的資料，將用來開發更具智慧的機器學習模型，而這些部署在物聯網上的模型，將透過採用人工智慧來創造良性循環。

具韌性的基礎設施

甚至在疫情襲擊前，快速復原的韌性(人為社會技術以及實體系統能夠吸收與抵禦突如其來之自然或人為衝擊的能力)早就存在印太地區許多人的腦海中。當《麻省理工學院科技評

論》(*MIT Technology Review*)雜誌2020年在達佛斯會議期間詢問專家如何預測2030年時，「3A學院」(3A Institute)院長兼澳大利亞英特爾(Intel)公司高級研究員貝爾(Genevieve Bell)回答道，未來將明白20世紀基礎設施有多麼欠缺韌性。貝爾指出：「吾人將被迫面對20世紀所有基礎設施──電力、用水、通信以及公民社會本身──都很脆弱的事實。而這種脆弱特性會使21世紀更難以支撐下去。」疫情僅是凸顯如此特點，而美國醫療保健基礎設施，在因應新冠肺炎的方式也只是一種(令人不安的)數位資料。另一例則是：儘管東南亞經常遭遇旋風襲擊，但該區域政府的因應措施卻仍然不足。

在實體基礎設施方面，專家通常將「智慧城市」(Smart Cities)，視為治療所有困擾城市生活環境的萬靈藥。例如，「東南亞國協」(ASEAN)就制定了「智慧城市網絡行動計畫」(Smart City Network Action Plan)且不論就城市而言，「智慧」由何構成，乃至智慧城市概念本身，均未見廣為接受的定義。從最低限度來看，智慧城市必然是具備網路化，及可協助城市因應交通管理乃至垃圾處理等挑戰之資訊與通訊技術的城市。

若著眼於該地區的未來預測，聚焦於智慧城市的發展將頗具意義──2018年，聯合國曾預測指出，泰半亞洲國家到2050年將有74%以上的人口居住在城市中。此外，物聯網設施的數量預期會有爆炸性成長，加諸空間計算帶來之可能性，還有印太地區具韌性基礎設施之新概念出現，其中人工智慧及其他自動化系統運用諸如網路驅動手機等具備早期預警監視系統之「日常」智慧裝置，針對地理空間數據所做的無縫整合，能在韌性有所助力。若聽起來很抽象，考慮另一種可能性，那就是政府能夠從地理上鉅細靡遺地區分確認易受即將來臨之衝擊(如傳染疾病爆發或惡劣天氣)影響的個人與團體，並將其引導至合適的救援設施(如醫院與掩蔽處)。

抗敵技術

打擊不實資訊的必要性，乃是多次出現在印太地區戰略議程上的關鍵議題。就許多層面而言，在許多與俄羅斯情報機構有關的單位，以肆無忌憚的方式透過社交媒體影響2016年美國總統大選，如此挑戰顯得眾所周知。如臉書等大型社交媒體，也因其網站與運用遭到某些行為者巧妙操縱，散播不實資訊以達特定政治目標，而遭到日益嚴格的審查。

然而，借助機器學習工具乃是以技術協助打擊意欲煽動暴力之不實訊息與言論傳播的方法之一。臉書及谷歌都已開發分別名為Deeptext及Perspective等由人工智慧發展而來的工具，以打擊線上挑釁與仇恨言論。儘管這些工具仍需大量「人類審查員」，才能獲得實際效果，精進發展仍持續進行。2020年6月，由英國「國防科技實驗室」(Defense Science and Technology Laboratory)委託歐洲蘭德公司所進行的研究顯示，機器學習計算法可以檢測出包括「俄羅斯網路暴民」(Russian trolls)在內的社交媒體惡意行為人士。臉書也依賴人工智慧檢測在其平臺上散播不實之新冠肺炎訊息，並使用機器學

習的因應之法來攔阻大量有關口罩、測試套件及其他與流行病相關物資的廣告。美國「國防先進研究計畫局」(Defense Advanced Research Projects Agency, DARPA)也大量投資研究「深偽」(Deepfakes，幾乎無法區分真偽的人工智慧生成影片與圖像)。

然而，若考慮那些試圖汙染及利用團體資料庫的惡意行為者，則包括深偽在內，不實資訊不過構成一半挑戰。研究人員對於「敵意機器學習」(Adversarial Machine Learning)的可能性愈發謹慎看待；亦即有些技術駭客及其他惡意玩家，很可能會利用機器學習模型，在形成與部署過程中攻擊其固有弱點。一項由產業專業人士與學術機構進行並置於該議題輔助教育課程之共同研究成果指出，「支持生產機器學習系統的方法，經常很容易在機器學習供應鏈中產生一些新漏洞」，而遭對手駭入。

這些包括針對供應鏈之訓練或推理——抑或兩者兼具的特定目標。「模型中毒」(Model Poisoning)乃是敵意機器學習攻擊的一種方式；攻擊者循此方式「汙染機器學習系統的訓練資料，以便在推理時獲得所欲結果」。一份產業報告指出，2022年發生的網路攻擊中就有三成是敵意機器學習。隨著物聯網導致人工智慧驅動系統的日益普及，將須持續研究敵意機器學習，並且進行國際合作。

重新審視緣由

如同之前所常言般，在「技術樂觀主義」(Techno-optimism)以及「技術悲觀主義」(Techno-pessimism)間，存在著「技術現實主義」(Techno-realism)。在如此背景下，筆者試圖朝兼具前瞻性與規範性的方向思考。基於對印太地區在需求及現有技術所處位置的當前趨勢推斷觀之，本文極具前瞻性。前述論點係在忽視規範立場的情況下描述極可能實現的情況。但本文仍可視為運作規範：假使區域國家持續期待自由、開放、包容且具韌性的印太地區，他們就可以在該區域進行一些有益甚至是非正式的合作。

然而，涉及國家與諸如商業實體之非國家行為者在國際技術合作方式，也具有強大的「制度外部性」(Institutional Externality)，因為據其使用的規範將更容易社會化。這轉而具有地緣政治功能。具體來說，就上述有關智慧監視以及韌性基礎設施的討論為例，顯見中國大陸追求人工智慧驅動監控，不僅影響其國內少數民族，還將該技術的運用「社會化」到世界各國，其中也包括眾所皆知的威權國家。然而，假若形成印太科技聯盟，並共同設計開發智慧監控及合乎道德的部署方式，而非呼籲各國避免使用智慧監控，就會自動成為制衡中共的強大力量。

結論：科技，甚至是人工智慧，均並非地緣政治競爭者持盈保泰的靈丹妙藥；國際政治的複雜度遠勝如此。然而，人工智慧的誘人之處在於，可在許多國家面臨挑戰時將大家凝聚在一起，並直接或間接地解決許多問題。