全球政治評論　*Review of Global Politics*

第六十五期（2019）No.65 頁 15-20

焦點評析

人工智慧與國際政治—理論與實踐的對話

Artificial Intelligence and International Politics – A Dialogue between Theory and Practice

姚宏旻 *Hon-Min Yau*
國防大學戰略研究所助理教授
Assistant Professor of the Graduate Institute of Strategic Studies
National Defense University

前言

自 2016 年由 AlphaGo 完勝南韓棋王李世乭的「人機對弈」後，開啟了人工智慧(Artificial Intelligence, AI)的商業應用時代，各項技術與日俱進；舉凡智慧音箱、聊天機器人(Chatbot)、智慧醫療，多種應用滲透到我們的日常。現在除了可以用 Facebook Messenger 在美國叫車、透過 Google Flight 利用人工智慧幫忙找便宜機票， 2018 年 12 月的台灣甚至發生第一起特斯拉(Tesla)自駕車車禍。人們倏然發現，遍地開花的人工智慧應用，已不再是過去學術名詞概念化的驗證，卻早已是融入人們生活作息，影響人類真實活動的具體實踐。

人工智慧與權力政治

在 21 世紀的數位時代，科技即是權力；隨著人工智慧成為顯學，國際政治(International Politics)的權力體系(Systems of power)-亦即主權國家(States)-也伴隨著這樣的權力變動而產生相對映作為，世界各國正逐漸將人工智慧列為科技發展重點政策。美國除於 2016 年 3 月由國家科學技術委員會草擬《國家人工智慧研究與發展策略計畫》(National Artificial Intelligence Research and Development Strategic Plan)致力構建人工智慧科研環境，更於同年 12 月發佈《人工智慧、自動化與經濟》(Artificial Intelligence, Automation, and the Economy)白皮書擘劃人工智慧發展願景。而中國大陸則於自 2017 年 7 月由國務院頒佈《新一代人工智慧發展規劃》，並宣示於 2030 年前建設「人工智慧全球創新中心」。俄羅斯總統普丁則於 2017 年 9 月直言表示：「人工智慧已在國家安全扮演至關重要的角色，占領人工智慧制高點的國家未來將能主宰世界」(A*rtificial intelligence is the future, not only for Russia, but for all humankind. It comes with colossal opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world.*)。

除此之外，2017 年 7 月中國大陸國務院更進一步發佈「新一代人工智能發展規劃」，同時表示「人工智慧已成為國際競爭的新焦點，人工智慧是引領未來的戰略性技術」，並直言期許於 2030 年時成為「成為世界領先水平」的「世界主要人工智慧創新中心」；美國則隨即於 2017 年 12 月「國家安全戰略」(National Security Strategy)闡述他國人工智慧發展對美國國家安全將產生極高之風險衝擊，並直言視中國大陸為其安全之主要「戰略競爭者」。山雨欲來風滿樓，國際各國間正進行著一場人工智慧的國際軍備競賽。

人工智慧的發展與應用

各國對於人工智慧的投入，主要著眼於這種能超越傳統自動化

(Automatic)處理功能，進而提升至自主化(Autonomous)的學習能力；人工智慧係指能賦予機器具備人類一般的認知(cognition)能力，並允許機器獨立自主的判讀與回應未知的狀況。就其運算能力而言，可概分為「弱人工智慧」(Weak AI)及「強人工智慧」(Strong AI)；「弱人工智慧」設計目的，主要在於處理任一特定且需高度智力運算的問題，例如 AlphaGo 能下棋，卻不會開車；而「強人工智慧」則希望達到與人類並駕齊驅的智慧，並具有全面且廣泛的推理及處理問題能力。當前人工智慧的技術雖越趨成熟，惟其發展主要集中在前者。

而就人工智慧運算邏輯而言，可簡化為感應模式(Sensing)、最佳化模式(Optimization)及行動反應模式(Action)三個組成。以特斯拉自駕模式而言，人工智慧透過車上遍佈之 GPS、影像辨識等感測器執行感應模式，隨時掌握週邊交通狀況，並透過最佳化模式，持續與各感測器更新電腦對真實世界之認知，最後藉由行動反應模式，計量最佳方案。隨著巨量資料(Big Data)、雲端運算(Cloud Computing)與量子電腦(Quantum Computer)的基礎科學技術的深化，機器自主化的程度大幅提升，也因此未來人工智慧運用於惡劣作業環境下已成為可能，特別就軍事層面運用而言，自主化智能作戰載台之普遍運用，將能減少各國軍事行動任務執行間，因作戰傷亡而產生之裹屍袋症狀(Bodybag Syndrome)，減輕社會對各國執政者所可能造成的政治壓力。

人工智慧的武器化(Weaponization)

傳統的軍事系統早已運用許多電腦輔助決策支援的運算模組，舉凡航跡追蹤(Tracking)、載台識別(Identification)、目標判斷(Discrimination)、任務交付(Assignment)及武器接戰(Engagement)，皆透過運用電腦系統強大自動化處理能力。但是傳統軍事系統採取規則判斷(Rule-base Structure)的設計架構，人員常需參與關鍵系統決策循環(Human in the loop)；也因此每當

系統之接收端變數一樣時，輸出端必然採取相同之回應行為 (the same behavior)。但是人工智慧的優點則在於「自主」決定，亦即在考量一連串輸入變數之預期發生機率後，系統將產出可能行動方案；但人工智慧特別的是，當接收端變數一樣時，輸出端並不會採取相同之行動方案，而是採取某一類型之回應行為(a range of behaviors)。

因此，伴隨當前高速電腦運算能力及大型儲存媒體成本的巨幅下降，人工智慧演算法將超越過去軟、硬體技術限制並賦予軍事武器載台更多自主學習能力。除過去軍事掃雷、拆彈等工作可透過人工智慧機制降低人員傷亡，致命的自主攻擊載台也將減低作戰人員常時間作業負荷並執行全年無休的戰鬥任務。近年為人知之具體實例有美軍於巴基斯坦、阿富汗及葉門的反恐作戰，透過長時間使用滯空無人載具執行監偵，並藉由持續分析武裝份子接觸的人員及特殊行為模式，無人載具能立即執行所謂的特徵打擊(Signature Strikes)，摧毀可疑目標；另一個著名的例子則是 2011 年據報為美國及以色列佈署之震網(Stuxnet)蠕蟲，該蠕蟲除成功滲透具氣隙網路（air-gapped network）安全設計的伊朗納坦茲(Natanz)核武設施，並透過智慧的目標選擇，鎖定指定了控制鈾濃縮離心設備(nuclear centrifuge)的工業電腦，拖延伊朗核子武器進程；震網蠕蟲的發展被視為網絡空間(Cyberspace)射後不理(fire and forget)網路武器的概念實踐。

人工智慧的未來挑戰

毫無疑問的，在可見的未來人工智慧技術的軍事化勢必越來越普遍。雖然短期間尚不會造成如電影、小說情節描繪般，世界末日的人機科幻大戰，然而新興技術的崛起必然對人類社會活動產生一定程度的衝擊，也因此許多新興問題正逐漸浮現，亟待國際關係學者思考未來走向。

首先，美軍過去使用無人機的經驗已引起部分國家人民的反感，人權主義者也高聲抵制這些殺人機器橫行，國際關係學者須積極思辨這些在陸

地、天空、水面及水下的人工智慧機器，未來當它們在執行軍事任務時，是否有權能獨斷的決定人類的存活，這樣的議題除涉及倫理(Ethic)及規範理論(Normative Theory)的深層探討，也須檢視對人類安全(Human Security)的風險。除此之外，國際社會也須思考構建人工智慧機器的國際行為規範，建立明確交戰準則(Rule of engagement)的可能，這些的議題則涉及人工智慧載台之軍事運用與武裝衝突法(Law of Armed Conflict)與人道救援法(Humanitarian Law)之調和，需要跨領域的整合探討。

其次，這同時延伸另一層次問題，如果共通的行為規範(Norms)難以達到，是否可抑制人工智慧軍事化技術的擴散。然而，誠如文章開頭所言，人工智慧的商業應用已越趨普及，許多技術亦具有軍民通用與軍民融和的特性，過度限制將阻礙科技進展，惟不作限制卻可能造成軍武擴散(Proliferation)，如何求取適當平衡？再者，如果單就各國軍事化人工智慧技術加以限制，是否反而會造成軍事系統人工智慧研發人才的流失，如此政府及軍事機關未來缺乏對系統安全設計知識的深耕，結果反而危及戰場週邊軍事及非軍事人員之安全。

最後是對人工智慧武器作戰模式的最佳化行為與運用準則研究。傳統軍事指揮官在早期作戰規劃階段，須事先對預劃運用的武器與目標地區之相互關係有清楚之計量。考量的問題包含，諸如：希望達到什麼樣的摧毀效果？選用武器摧毀範圍是否會造成不必要的附帶損害(Collateral Damage)？選用的武器火力是否會對目標物週邊民用設施，如醫院、學校產生過分損害？在傳統武器的作戰模式上，過去由於這些武器之自動化程度低，指揮官往往須同時透過情監偵手段建立戰果評估(Battle Damage Assessment)，以能對前述問題有著較明確掌握。但就自主型的人工智慧武器而言，預判未來將帶來許多挑戰；以前述震網蠕蟲為例，自它被佈署至伊朗內部網路那一刻起，由於缺少跨越氣隙網路的偵察技術，作戰指揮官便須完全仰賴震網的自主作戰決定，無法掌握該武器作戰行動是否成功攻

擊授權目標？是否造成不必要附帶損害？職是之故，無論公開文獻上如何宣稱著震網已造成核設施損傷，並延緩伊朗核武計畫進程，但實際的損傷程度，恐怕只有伊朗政府本身才知道。也因此未來如何掌握這些自主武器所能造成的政治風險，將是軍事研究的重要課題。

結論

人工智慧是一把雙面刃。儘管新科技對於人類社會活動產生不可避免的影響，然而我們尚不需視科技對社會衝擊為不可逆的單向，並過度消極解讀人工智慧所帶來的未來。事實上，人工智慧強大的機器學習與運算能力，反而可能為人類未來之生存與發展賦予新的契機，協助對抗 21 世紀人類面臨的存在威脅(Existential Threat)。就如同火可以幫助人類烹煮食物，但也能會燒傷我們一般；新科技的本質並不代表善或惡，這完全取決於人們如何選擇使用它。也因此透過不斷社會建構的過程，人類社會仍具有重塑科技用途的能力；人工智慧或許會像 2018 年英國劍橋分析公司(Cambridge Analytic)「濫用」科技般，影響民主體制之選民抉擇；但人工智慧也具有無限潛能，可以受到「善用」，協助判讀醫療資料醫治疾病，甚至是幫助各國應對全球氣候變遷挑戰。

責任編輯：陳臻