AI：操控認知戰場

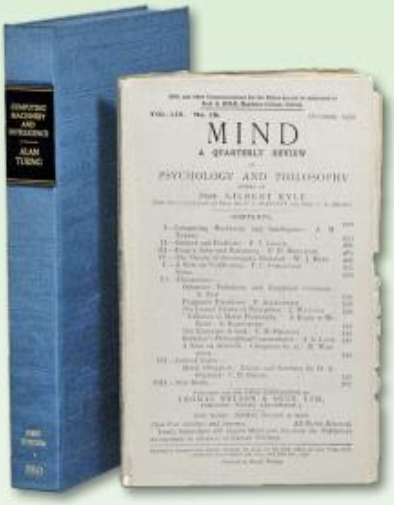
◆ 商業發展研究院副研究員 — 林士清

《孫子兵法》認為致勝關鍵在於以征服人心為上策；而現今 AI 技術完全可以擾亂資訊判讀，影響人心走向。

AI 技術誕生，衝擊人類「認知空間」

所謂人工智慧（AI），乃是指電腦、機器、程式，可透過模擬人類心智，自主學習來獲得解決問題及決策的能力。關於 AI 發展，可追溯至 1950 年英國科學家圖靈（Alan Turing）論文：〈運算機器與智慧〉（Computing Machinery and Intelligence），此篇論文衍生出所謂的「圖靈測試」（Turing Test）。該測試用來判斷電腦是否具有智慧，「如果一臺機器能夠與人類展開對話（通過設備）且不會被辨別出其機器的身分，那麼可稱這臺機器具有智能。」

AI 技術誕生，象徵人類科技可進一步模擬、延伸及擴展人類智能。從科學演化歷史來看，在 1970 年代，AI 也曾因不受主流社會支持而步履蹣跚，後來憑藉硬體技



英國科學家圖靈於 1950 年發表〈運算機器與智慧〉論文，衍生出「圖靈測試」的概念。（Photo Credit: Manhattan Rare Book Company, https://www.manhattanrarebooks.com/pages/books/2063/alan-turing/computing-machinery-and-intelligence-in-mind?soldItem=true）

「圖靈測試」主要用來判斷電腦是否具有智慧，如果一臺機器能與人類展開對話且不被辨別出其機器的身分，那麼就可稱這臺機器具有智能。

術的全方位提升和互聯網大數據的積累而得到突破性的發展。AI 以人工神經網絡的研究為基礎，以機器學習為主要特徵，因深度學習算法和演算力的重要突破，在諸多應用領域都取得可觀成果。不過，對於社會科學家來說，AI 對於區域政經局勢帶來的衝擊尚未清晰可知。

例如，「灰色地帶」（Gray zone）衝突，意旨在「虛擬空間」、「網路空間」、「認知空間」等的戰爭型態，乃是近年來運用 AI 來影響國家安全的流行名詞，常與「認知作戰」（Cognitive warfare）或「混合戰」（Hybrid warfare）等語境所互用。當國家試圖運用各種非軍事手段，以達成其國家政策目標，訴諸之行動有時是非戰爭的軍事行動，此行動雖未動用到真槍實彈，然已對目標國家造成威脅。

AI 技術操縱「認知空間」戰場

未來戰場不僅包含「物理空間」，即海上、陸地、空中、太空這樣的「自然空間」，甚且包括「虛擬空間」—即「網路空間」和「認知空間」。「認知空間」指由人類情感、思維、意志、信仰和價值觀等構成的空間。因此，在「認知空間」作戰，並非僅指如駭客般地竊取或破壞「網路空間」，而是先藉由在「網路空間」中取得話語權優勢（即資訊流道管道，如網路媒體等），再經由「網路空間」而攻占人腦的「認知空間」，以爭奪人心的支持。

《孫子兵法》：「上兵伐謀，其次伐交，其次伐兵，其下攻城。」即孫子認為致勝的關鍵在於人心的攻防，要以征服人心為上策，而現今**AI技術完全可以擾亂資訊判讀，影響人心走向**。

威權國家熱衷AI技術發展

北京施行威權體制，此種支配與主導的全面性關係已造就「強國家、弱社會」現狀，造成政治上對人民權利的限縮、經濟上對市場的不當的介入與干涉、社會上對人民團體的動員及反動員、教育上深化對意識型態的塑造，以及文化上的強勢之唯我獨尊。觀諸世界，威權體制國家對AI技術發展又顯得最為熱衷，主要原因在於其能對人民實施有效控管。

多年來，中共一直在開發AI技術，包括人臉識別系統，監控每個人的一舉一動，還可以預測某個人下一步可能會做什

未來戰場不僅包含「物理空間」，甚至包括「虛擬空間」，其指透過網路攻占人腦的認知，藉此影響人類情感思維與價值觀。

華為和臉部辨識公司曠視曾合作測試AI監控系統，其能在人群影像中，自動識別出個體的年紀、性別與種族，並配有「維族告警」，一旦該系統自人群中鑑別出突厥裔臉孔，就會立即通知監控單位。（Source: IPVM, https://youtu.be/8aMyVkYtMFQ）

麼，是否會對政府構成威脅等。《華盛頓郵報》曾報導，華為和臉部辨識公司曠視（Megvii）曾合作測試一組 AI 監控系統，能在人群影像中，自動識別出每個個體的年紀、性別與種族，並配有「維族告警」（Uyghur alarm）；一旦該系統自人群中鑑別出突厥裔臉孔，就會立即通知監控單位。訊息研究公司 Comparitech 於 2022 年 7 月報告指出，中國大陸境內共部署 5.4 億架監控攝影機，幾乎每 2 個中國人就被 1 個監控攝影機盯著。[1] 足證 AI 技術已可全面協助威權政體實施社會控制，而我們正在親眼目睹一個「科技極權治理模式」的時代誕生。[2]

AI 控制資訊流的方式

AI 發展至今，已被掌權者用來作為鞏固政權或對外擴張的工具多年，尤其是威權政體，經常藉由無上限的預算進行資訊流控管，更讓全球民主國家政府非常擔憂。

目前 AI 技術最常用來控制資訊流通的方式如下：

首先

「阻斷」，乃是 AI 能強化訊息隔絕措施，如過濾敏感內容、屏蔽關鍵字詞等。當兩軍對峙時，不符合一方所需的新聞資訊，皆應該大規模地被該方屏蔽；因為無法被阻斷的訊息四處亂竄，只會讓人心惶惶、影響作戰士氣。

[1] 中央社，《中國監控攝影機全球最多 估每 2 人被 1 鏡頭監視 專家：AI 極權王國》，https://www.cna.com.tw/news/acn/202208280079.aspx。

[2] 轉角國際，《電馭新疆的『AI 暴政』：中國數位恐怖的維吾爾監控再進化》，https://global.udn.com/global_vision/story/8663/5102799。

北京當局時常以綜合型態的認知作戰讓臺灣內部不同族群互相對立，經貿利誘與限制即為其中之一，如設法禁止臺灣產品進口中國大陸。（圖片來源：行政院，https://www.ey.gov.tw/Page/9277F759E41CCD91/7cdeb686-ddf6-4b88-85a2-a4d8d224c109；中華人民共和國海關總署，https://ciferquery.singlewindow.cn/）

《孟子》〈離婁篇〉：「今之欲王者，猶七年之病，求三年之艾也，苟為不畜，終身不得。」此段談話經常被引喻為凡事應預先做好準備，臨渴掘井終究是緩不濟急。當受眾收到假訊息並信以為真時，便會影響其行為，從溫和轉向激進而造成內部動亂；切莫「敵人尚未攻打，內部先自毀長城」，甚至如吳三桂大開城門，引清兵入關。因此，政府因應假訊息氾濫，不論採取立法查察、建立訊息下架或示警機制、主動揭露調查結果或完善第三方事實查核機構等，應以避免假訊息如同病毒般在第一時間快速傳播為第一考量。尤甚，能否避免 AI 帶來的資訊誤判，從而導致難以挽回的戰爭局面，更考驗著兩岸領導人的智慧與耐性。和平，方為萬世之福。

中共近期頻繁在臺灣周遭海域進行空中偵察、海上巡演，皆被視為是灰色地帶手段，讓臺海兩岸對峙緊張情勢持續升高。（圖片來源：國防部發言人 FB，https://www.facebook.com/photo/?fbid=526323593005458）