

# 俄烏戰爭中人工智慧科技之應用態勢 及其戰略意涵

## Application and Strategic Implications of Artificial Intelligence Technology in the Russia-Ukraine War

張凱銘

台中科技大學通識教育中心

kaiming0149@nutc.edu.tw

### 壹、前言

2022 年 2 月 24 日爆發的俄羅斯與烏克蘭戰爭（Russia-Ukraine War，下簡稱俄烏戰爭），如今看來很可能將成為二十一世紀影響最為深遠的重大國際事件之一。這場戰爭將交戰實況與血腥景象透過資訊傳媒即時遞送至全球民眾面前，使人們清晰察見現代戰爭的殘酷與巨大破壞力。而後冷戰時期的國際地緣政治格局也隨著戰爭爆發而呈現深層重組趨勢，美國、中國、俄羅斯與歐洲聯盟（European Union, EU）等重要行為體間的關係及實力對比正出現微妙變化。

對於國際關係學界而言，這場迄未落幕的戰爭似乎有效帶動了許多饒富意義的研究議題，除相關國家的國防戰備和外交政策動向備受矚目外，歐洲區域整合前景、能源供應作為外交工具的戰略意涵，以及由戰爭所衍生的糧食危機、人道災難與通貨膨脹加劇效應

等問題，都廣受各國專家學者關注。在眾多影響之中，俄羅斯、烏克蘭及其他牽涉國家如何在這場戰爭中實地應用人工智慧（Artificial Intelligence，下簡稱 AI）技術是一項饒具探索價值的重要議題。就當前發展情勢以觀，這場戰爭似乎正成為歷史上應用 AI 最為廣泛深入的一場軍事衝突，對於未來的戰爭型態及 AI 後續發展方向，很可能將造成深遠影響。

對此，本文在以下篇幅中首先將檢視有關國家在俄烏戰爭過程中如何實際應用 AI 技術，其次則就該技術的防務運用狀況提出省思與前景評估，最後，則嘗試就俄烏戰爭中 AI 應用的戰略意義和啟示作出總結。

## 貳、俄烏戰爭中的 AI 技術應用態勢概覽

AI 技術發展可回溯至 1940 年代的機器學習（Machine Learning）研究，此後，得益於神經網路（Neural Network）與深度學習（Deep Learning）研究法先後興起、個人電腦設備廣為普及、硬體運算效能逐漸提升，以及網際網路創造大量可用數據等有利條件，該技術在進入 21 世紀後迅速成熟。

各界在注意到 AI 可能創造巨大經濟效益與社會變革的同時，也對於軍用 AI 的演進趨向漸有關注。例如，美國國家科技委員會（U.S. National Science and Technology Council）與總統行政辦公室（Executive Office of the President）於 2016 年 10 月聯名發表的政策文件《準備迎接人工智慧未來》（*Preparing for the Future of Artificial Intelligence*）中，便在討論 AI 帶動自動化經濟發展的同時，以專節探討該技術應用於國防事務與軍事武器研發的優勢和潛在風險。<sup>1</sup>

---

<sup>1</sup> U.S. National Science and Technology Council & Executive Office of the President,

時至 2021 年 5 月，以色列向巴勒斯坦發起的所謂「圍牆守衛行動」(Operation Guardian of the Walls)，為世界各國展示了 AI 在戰爭中的顯著價值。在這場為外界稱為史上「第一次 AI 戰爭」(the first artificial-intelligence war) 的軍事行動中，以色列軍方將該技術應用於強化飛彈攔截系統運作效能、即時偵察敵軍動向，辨識戰場攻擊標的與提高打擊精確度等面向，並且皆取得了相當亮眼的成果。<sup>2</sup>至於 2022 年 2 月爆發的俄烏戰爭，則進一步擴大了 AI 的軍事應用範疇，俄羅斯、烏克蘭及包含美英等國在內的烏國友邦，在這場戰爭的許多環節都不同程度的使用了 AI，堪稱 AI 技術應用最為廣泛的一場戰爭。

綜觀各方作為，AI 技術在這場戰爭中的應用途徑可概括為「戰術攻防」、「情報工作」與「決策輔助」等三者，於下分別說明：

#### 一、戰術攻防

AI 在俄烏戰爭中最直接的用途當屬俄羅斯與烏克蘭政府雙方使用此技術展開的激烈攻防交戰。作為當代國際體系中的主要大國行為體，俄羅斯在先進 AI 研發進程方面雖然落後於美國與中國，但其軍工產業對於配置 AI 技術的無人載具及自動化武器系統的開發已頗有成就。美國海軍分析中心 (CNA Corporation) 便指出，俄羅斯軍方對於無人機的戰術運用能力已達相當程度，主要用於戰場偵察與火力打擊之中，同時也積極探索無人車輛、無人水面航行器及潛航器

---

*Preparing for the Future of Artificial Intelligence* (Washington, D.C.: U.S. National Science and Technology Council, 2016), pp. 29-38.

<sup>2</sup> Anna Ahronheim, "Israel's Operation Against Hamas was the World's First AI War," *The Jerusalem Post*, MAY 27, 2021, <https://www.jpost.com/arab-israeli-conflict/gaza-news/guardian-of-the-walls-the-first-ai-war-669371>

的實戰應用可能。<sup>3</sup>在此次俄烏戰爭中，俄軍於 2022 年 3 月展開基輔攻勢時，便曾經投入其自製的 KUB-BLA 無人機。值得注意的是，烏克蘭的 AI 武器自製能力雖不及俄方，但在本次戰爭中也使用了土耳其製造的 TB2 無人機。<sup>4</sup>上述機種皆配置自動化導航跟蹤、AI 視覺辨識 (Artificial Intelligence Visual Identification, AIVI) 等功能，可以自主監控、識別與打擊目標，除可降低人員傷亡風險外，也有利於提升攻擊效率。<sup>5</sup>

除了戰場上的火力打擊外，AI 技術在這場戰爭中也被運用於數位層面的網路系統防禦。美國微軟公司 (Microsoft Corporation) 一份以俄烏戰爭為研究對象的調查報告《保衛烏克蘭：網路戰爭的早期啟示》(*Defending Ukraine: Early Lessons from the Cyber War*) 中便指出，俄羅斯控制的駭客團體在交戰過程中曾試圖滲透數百萬台電腦，規劃向 48 個烏克蘭政府與民間機構發動網路攻擊，但因烏國及其友邦透過 AI 技術的監測分析事先掌握威脅情報，得以預先部署防禦措施，並關閉電腦系統中的潛在惡意程式，有效抵禦了這場攻擊威脅。<sup>6</sup>

而在戰場後方，AI 對於強化經濟制裁效果同樣有所助益，例如以金融交易 AI 監測技術為主要業務領域的 ThetaRay 公司，便向英美

---

<sup>3</sup> CNA Russia Studies Program, "Russian Military Continues Using UAVS in Reconnaissance Strike and Fire Contours," *Artificial Intelligence and Autonomy in Russia*, No. 43 (August 2022), pp. 3-6.

<sup>4</sup> Will Knight, "Russia's Killer Drone in Ukraine Raises Fears About AI in Warfare," *WIRED*, March 17, 2022, <https://www.wired.com/story/ai-drones-russia-ukraine/>

<sup>5</sup> 關於相關機種的配置與功能資訊，請參考：Army Technology, "Zala KYB Strike Drone, Russia," March 25, 2022, <https://www.army-technology.com/projects/zala-kyb-strike-drone-russia/>；BAYKAR Technology, "Bayraktar TB2," <https://www.baykartech.com/en/uav/bayraktar-tb2/>

<sup>6</sup> Microsoft Corporation, *Defending Ukraine: Early Lessons from the Cyber War* (Redmond: Microsoft Corporation, 2022), p.2.

等國家提供服務，運用 AI 技術自動偵測追蹤俄方可疑的金錢流向與交易活動，同時鎖定被列入制裁名單行為者的資金和商業動向，藉以阻止俄羅斯政府及其企業轉移資金迴避經濟制裁。<sup>7</sup>

## 二、情報工作

AI 技術在俄烏戰爭中也被廣泛應用在情報工作之上。長期提供美國情報部門技術支援的 AI 企業 Pirmer，其開發的 AI 演算法便在本次戰爭中為美方運用於自動記錄、翻譯、篩選、分析俄羅斯士兵在未加密頻道的無線電通訊內容，藉此評估俄軍戰場動向與部隊士氣等實況。<sup>8</sup>

另一方面，AI 在俄烏戰爭中展現其兼具使情報資訊清晰化與混沌化的雙重功能。在清晰化部分，AI 技術的臉部辨識功能為烏克蘭軍方與部分民間團體用於查核確認俘虜身份，以及辨認出現於新聞畫面中特定不明人士的背景，例如現身俄方軍事高層行列或政府活動場合畫面中的某張陌生面孔。臉部辨識還有利於防範俄羅斯情報部門對烏克蘭及其友邦的滲透，使各國反情報部門能夠更精準掌握俄方情報人員真實身份，提高其執行潛伏工作的難度。<sup>9</sup>

除此之外，臉部辨識技術也被用於遺體查對，烏克蘭國防部與

---

<sup>7</sup> Rochester First.Com, "ThetaRay AI Tech Enables Financial Institutions and Regulators to Identify Illicit Attempts to Circumvent Economic Sanctions," March 02, 2022, <https://www.rochesterfirst.com/business/press-releases/cision/20220302LN79235/theta-ray-ai-tech-enables-financial-institutions-and-regulators-to-identify-illicit-attempts-to-circumvent-economic-sanctions/>

<sup>8</sup> Sean Gourley, "A New Era of Warfare: How AI Unlocks Intelligence from Russian Radio Chatter in Minutes," *Pirmer*, April 4, 2022, <https://primer.ai/public-sector/a-new-era-of-warfare-how-ai-unlocks-intelligence-from-russian-radio-chatter-in-minutes/>

<sup>9</sup> James Clayton, "How Facial Recognition is Identifying the Dead in Ukraine," *BBC*, April 13, 2022, <https://www.bbc.com/news/technology-61055319>

美國 Clearview AI 公司合作，運用該公司的辨識服務，交叉比對戰場身分不明遺體相貌，與臉書（Facebook）、推特（Twitter）等社交媒體上的用戶照片，藉以找出陣亡俄軍真實身份並通知其家屬領取遺體。烏克蘭副總理兼數位轉型部長費多羅夫（Mykhailo Fedorov）指出，這樣做既能讓陣亡者家屬知悉實情，也有助於打破俄羅斯政府對外宣稱這場戰爭僅派職業軍人參戰且幾無傷亡的假象。費多羅夫也透露，烏國在戰爭中得到許多西方科技企業的支持，包括他主持的數位轉型部也正使用亞馬遜公司（Amazon）的雲端儲存技術保存關鍵資料。<sup>10</sup>

在資訊混沌化部分，可以參考的案例當屬俄羅斯政府在戰爭中利用 AI 生成大量深偽（Deepfake）影像，再透過抖音（TikTok）等網路影音傳媒對外散播澤倫斯基（Volodymyr Zelenskyy）總統投降、蛇島（Snake Island）駐防官兵全數陣亡等訊息，藉以擾亂外界對於戰事走向的判斷，並打擊烏克蘭及其友邦的信心與前線官兵士氣。<sup>11</sup>烏克蘭國安單位也指控俄羅斯利用網路機器人帳號（bots）在社交媒體上散播不實的戰爭訊息試圖引發群眾恐慌。<sup>12</sup>不過烏國自身似乎也利

---

<sup>10</sup> Paresh Dave and Jeffrey Dastin, "Exclusive: Ukraine has Started using Clearview AI's Facial Recognition During War," *Reuters*, March 15, 2022, <https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ai-facial-recognition-during-war-2022-03-13/> ; Greg Ip, "Big Tech Is the West's Surprise Weapon in Competition with Russia, China," *The Wall Street Journal*, August 3, 2022, <https://www.wsj.com/articles/big-tech-is-the-west-s-surprise-weapon-in-competition-with-russia-china-11659535233>

<sup>11</sup> BBC News, "Ukraine War: False TikTok Videos Draw Millions of Views," April 25, 2022, <https://www.bbc.com/news/60867414>

<sup>12</sup> Esther Ajao, "AI and disinformation in the Russia-Ukraine war," *TechTarget*, March 14, 2022, <https://www.techtarget.com/searchenterpriseai/feature/AI-and-disinformation-in-the-Russia-Ukraine-war> ; Noor Ibrahim, "We are not Prepared': Russia uses Artificial Intelligence, Deep Fakes in Propaganda Warfare," *Global News*, March 30, 2022, <https://globalnews.ca/news/8716443/russia-artificial-intelligence-deep-fakes-propaganda-war/>

用相類技術合成影片偽稱戰果以求提振士氣。<sup>13</sup>

### 三、決策輔助

AI 技術在這場戰爭中似乎也被應用於輔助決策者判斷戰場情勢與戰情可能走向。例如網路企業 **Seekr Technologies** 與長期經營商務 AI 軟體應用的 **Semantic AI** 公司建立合作關係，運用前者的搜尋引擎技術大量且持續地蒐集和俄烏戰爭有關的各種公開資訊，包括新聞報導、各方政府官員發言等，再透過後者的 AI 軟體比對分析資訊內容，藉以發掘並排除相關資訊可能蘊含的誇大不實與刻意誘導成份，篩選出真實可信的情報，並提供給美國政府作為相關部門的決策參考。

前述這種情資蒐集過濾的工作雖然也可以由專職人員手動操作完成，但使用 AI 技術處理，很明顯的在執行效率、穩定度與成本方面都有更優秀的表現。除此之外，使用 AI 蒐集評估公開資訊，還兼有呈現各方行為體間內在脈絡的重要價值：AI 技術經由持續運算比對各方發送的種種資訊，可逐漸勾勒出不同人物、機構、黨派、部門或國家之間隱藏的脈絡連結，可有效抵消特定國家試圖藉由分散訊息傳播管道，利用潛在協力者供給資訊以誤導他國的努力，使政府決策者盱衡局勢時能更清晰地洞察全盤態勢，進而做出合理的行動判斷。<sup>14</sup>

---

<sup>13</sup> Michael Trobridge, "Fact check: How to spot a fake military success story in Russia-Ukraine war," *Deutsche Welle*, April 13, 2022, <https://www.dw.com/en/fact-check-how-to-spot-a-fake-military-success-story-in-russia-ukraine-war/a-61453500>

<sup>14</sup> Cision PR Newswire, "Seekr Technologies is Selected by Semantic AI for Joint Project that Exposes Russian Threats During Ukraine Crisis," March 22, 2022, <https://www.prnewswire.com/news-releases/seekr-technologies-is-selected-by-semanti-c-ai-for-joint-project-that-exposes-russian-threats-during-ukraine-crisis-301508113.html>

### 參、俄烏戰爭中 AI 技術應用帶來的省思

AI 技術在 2022 年俄烏戰爭中的實地應用狀況，有力地說明這項科技在國家安全和軍事行動中具有極高的價值，不論是戰場攻防進退、戰場外的情報分析，或是決策端的情勢研判，AI 都能發揮很好的支援作用，具有全面向的應用價值。而此一案例也展現出 AI 技術未來在國家安全層面的幾項可能發展趨勢，包含產官學協力推進技術發展的必要性、技術依賴可能衍生的脆弱性問題，以及該技術對強權競逐的關鍵影響等。

首先，俄烏戰爭作為近年國際間最受矚目也最為「透明」的一場戰爭，各國政府必然從中洞見 AI 的防務價值。考慮到掌握技術領先地位某種程度上即意味著取得軍事優勢，可以想見許多國家未來將更有意願擴大投資 AI 創新研發，積極嘗試將其投入各種軍事用途，AI 由此將成為軍備競賽的新興熱點領域。

然若由效率層面來看，這類新興資訊科技的發展似乎不宜由政府部門全盤主導，來自學術機構和產業界的研發創新往往更具動能及活力，與其由政府下轄單位獨力負責 AI 開發工作，採取產官學三方協力模式可能是更為聰明的選擇。美國政府近年發表的國家科技戰略規劃中對此便多有著墨，強調將建立政府單位與產業界與高等教育機構間的技术分享和人才流動，並探索在防務體系中擴大導入民間產業的商用現貨產品（Commercial off the Shelf, COTS）以提升研發效率及降低成本的策略路徑，期望藉由相關努力鞏固美國在先進資訊領域的領先優勢。<sup>15</sup>

---

<sup>15</sup> U.S. Department of Defense, *Summary of the 2018 Department of Defense Cyber Strategy* (Washington, D.C.: U.S. Department of Defense, 2018), p. 4; U.S. Department of Commerce and U.S. Department of Homeland Security, *A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce*



其次，AI 技術固然可為現代國家的防務工作提供諸多輔助，但一體兩面的問題是當一國的國防體系對 AI 依賴越是深入，在享受其創造的效能和便利性時，其科技運作鏈結遭遇對手惡意打擊並產生嚴重損害的風險及脆弱度也就同步增高。

具體而言，敵對國家若能針對晶片供應、衛星運作、行動通訊服務或雲端運算系統等技術環節施加打擊，就可能對國家的 AI 運算能力造成衝擊，進而損害其防務能力。例如俄羅斯在 2022 年 2 月 24 日發起對烏克蘭的軍事行動數小時之前，便搶先一步對衛星通信公司 Viasat 部署於歐洲和中東地區的衛星系統實施網路攻擊，使烏克蘭與歐洲多國的網路服務遭受影響陷入混亂。<sup>16</sup>因此，國家在積極推動 AI 防務應用的同時，亦應清楚認知到技術依賴可能衍生的脆弱性問題，同步加強對資安防護技術開發工作的經略。

最後，由於 AI 不論在軍事、情報、經濟發展與民生服務等方面都具有極高的應用價值，其逐漸成為牽動國際關係與各國國力消長的關鍵所在。

綜觀目前國際情勢，美國與中國的抗衡競爭仍是牽動外交事務的核心要素，而這兩個國家既是當前國際間最具軍事及政經影響力的強國，也是 AI 領域領先強權。例如英國《慢傳媒》(Tortoise Media) 2020 年末發表的《全球人工智慧指數報告》(Global AI Index) 中便指出，美中兩國的 AI 綜合實力高居全球排名的第一、二位；<sup>17</sup>史丹佛大學人本人工智慧研究院 (Stanford Institute for Human-Centered

---

(Washington, D.C.: U.S. Department of Commerce & U.S. Department of Homeland Security, 2018), pp. 1-20.

<sup>16</sup> Patrick Howell O'Neill, "Russia Hacked an American Satellite Company one Hour before the Ukraine Invasion," *MIT Technology Review*, May 10, 2022, <https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/>

<sup>17</sup> Tortoise Media, *Global AI Index* (London: Tortoise Media, 2020), pp. 1-6.

Artificial Intelligence) 在《2021 年人工智慧指數報告》(*Artificial Intelligence Index Report 2021*) 中也得到相同的評估結論。<sup>18</sup>

美國政府對於中國 AI 技術實力的迅速崛起已有警覺，<sup>19</sup>而俄烏戰爭體現的 AI 戰略價值，勢將進一步堅定華府當局強化在此領域制衡中國的決心。美國政府近年持續加強管制晶片等高階科技產品向中國輸出，<sup>20</sup>同時嚴密防範中方透過「千人計劃」等管道挖角高科技專業人才。<sup>21</sup>在監管措施持續加強的情況下，中國未來在 AI 領域的技術發展或將因為缺乏高階人才培育能力與技術獨立性而逐漸面臨困難，例如硬體設備運算效能遭受限制，以及落後於 AI 演算法更新進程等。在這種情況下，AI 或將成為決定美中競逐勝負的關鍵因素之一。

#### 肆、結語

2022 年俄烏戰爭的爆發為疫情下充滿不確定性的國際政局再添變數，也直接導致了各種人道災難與糧食、能源供應與經濟衰退等

---

<sup>18</sup> Stanford Institute for Human-Centered Artificial Intelligence, *Artificial Intelligence Index Report 2021* (Stanford: Stanford University, 2021), p. 17.

<sup>19</sup> U.S. National Security Commission on Artificial Intelligence, *Final Report* (Washington, D.C.: U.S. National Security Commission on Artificial Intelligence, 2021), p. 20.

<sup>20</sup> Karen Freifeld and Alexandra Alper, "Exclusive: Biden to hit China with Broader Curbs on U.S. Chip and Tool Exports-Sources," *Reuters*, September 16, 2022, <https://www.reuters.com/business/exclusive-biden-hit-china-with-broader-curbs-us-chip-tool-exports-sources-2022-09-11/>

<sup>21</sup> Ellen Barry and Gina Kolata, "China's Lavish Scientific Funds Fall into Prosecutors' Spotlight," *The New York Times*, February 7, 2020, <https://www.nytimes.com/2020/02/06/us/chinas-lavish-funds-lured-us-scientists-what-did-it-get-in-return.html>

多重衍生效應。然而對於 AI 的技術發展來說，俄羅斯、烏克蘭及相關國家在戰爭中對 AI 的全面應用，使世人完整認識這項技術的防務價值。

隸屬美國智庫「戰略暨國際研究中心」(Center for Strategic and International Studies, CSIS)的人工智慧治理計畫(Artificial Intelligence Governance Project)負責人艾倫(Gregory C. Allen)指出，對於軍用 AI 技術開發工作來說，缺乏足夠數量的數據資料供其改良演算法始終是最大阻礙。就這點來看，俄羅斯對烏克蘭發動的侵略戰爭固然是場災難性的悲劇，卻也使得俄方及北約各國得到了實際操作軍用 AI 技術產品，從中回收實務數據的珍貴機會。<sup>22</sup>

隨著 AI 的防務價值在本次戰爭中大為突顯，各國之間的 AI 軍備競賽料將持續升溫，在可預見的未來中，相關國家或將「把握」每一場武裝衝突與戰爭情境，擴大應用各種 AI 技術以求加速研發進程，俾掌握相對優勢。換言之，AI 技術在戰爭中的應用將逐漸常態化，為避免情勢失控，各國有必要同步推進 AI 軍備管制，以及軍用 AI 倫理標準等議題。

---

<sup>22</sup> Gregory C. Allen, "Russia Probably Has Not Used AI-Enabled Weapons in Ukraine, but That Could Change," *Center for Strategic and International Studies*, May 26, 2022, <https://www.csis.org/analysis/russia-probably-has-not-used-ai-enabled-weapons-ukraine-could-change>

