DOI:10.6237/NPJ.202510_59(5).0008

論「數位灰色地帶」的「認知戰」與反制之道

Cognitive Warfare：The Fight for Gray Matter in the Digital Gray Zone

作者：美國空軍中校麥可・奇塔姆(Michael J. Cheatham)等四人，奇塔姆為美軍聯合參謀部安全辦公室副主任。
譯者：劉宗翰中校。

本篇取材自美國《聯合部隊季刊》(Joint Force Quarterly)，2024年第三季，本文屬公開出版品，無版權限制。

提　　要：

一、俄羅斯與中共持續運用「數位灰色地帶」向美國及其民主國家發動「認知戰」，企圖在不發一槍一彈情況下，影響對方的認知判斷與決策過程，這已成為一種新的戰爭形式，各國軍方應審慎看待這種型式的戰爭所帶來的破壞力與影響。

二、「知己知彼，百戰不殆」。本文分析俄羅斯與中共在認知領域的部署，揭示其策略、操作手法和案例，及雙方意在對美國造成的「功能性失敗」，藉此扭轉傳統武力位居下風的弱勢，這也意味著民主國家必須強化「認知戰」的辨識與防禦力，才能維護國家安全與社會穩定。

三、為因應「認知戰」的威脅，作者提出反制之建議，分別是高層重視、強化官兵教育及排定周期性訓練；強化媒體素養；發展防禦機制，也就是認知安全唯有整合教育、科技與心理層面，如此才能有效建立面對「認知戰」的整體防禦作為。

關鍵詞：認知戰、反身控制、三戰、數位灰色地帶

壹、前言

美國正面臨前所未有的認知領域挑戰，民主國家在建立集體理解與共識的過程中舉步維艱；而俄羅斯與中共卻持續在「數位灰色地帶」向美國及其他民主國家發動「認知戰」。由於這些「認知戰」的戰術都是未達戰爭程度，導致無法以軍事行動方式加以回應。誠如克勞塞維茨(Carl von Clausewitz)在《戰爭論》(On War)所言，「戰爭是意志力的競爭」，戰爭本質在於克服和瓦解敵方意志；換言之，現代

戰爭不僅是陸、海、空的實體領域，影響並操控對手的認知與決策過程也同樣重要，「認知戰」儼然成為一種新的戰爭形式。

鑑此，本文架構將優先檢視認知領域構成的挑戰，接著探討「認知戰」的攻防與俄羅斯、中共在認知領域的部署，並指出當前「數位灰色地帶」(Digital Gray Zone)已成為「認知戰」的戰場，並從中分析人的認知特質與心理弱點，最後亦提出反制「認知戰」的因應之道。本文目的在說明「認知戰」構成的挑戰不容小覷，揭示「數位灰色地帶」如何成為認知操弄的主要場域，以及人類認知特質在俄、「中」兩國認知操控下所暴露的弱點，並提出具體可行的建議，以協助民主國家強化認知領域的防衛韌性與應變能力。

貳、認知領域的挑戰

一、根據「北約盟軍轉型司令部創新中心」(NATO Allied Command Transformation Innovation Hub)的創新項目負責人弗朗索瓦・杜・克呂澤爾(François du Cluzel)指出，認知領域有下列幾個關鍵特點：

(一)「認知戰」(Cognitive Warfare)會讓人難以理解事情、無法產生新知識，甚至讓錯誤資訊不斷浮現，並混淆人的判斷。

(二)認知科學涵蓋所有與知識形成及處理有關的學科，如心理學、語言學、神經生物學、邏輯學等。

(三)「認知戰」係利用知識來達成對抗之目的，廣義來說，「認知戰」並不侷限於軍事領域或某個體制，自1990年代初以來，這種能力開始被用於政治、經濟、文化與社會等領域。

(四)現代資訊技術的每一位使用者都是潛在目標，「認知戰」針對的是整個國家的「人力資本」(Human Capital)。[1]

二、利用「認知戰」來針對一國的人力資本，正是一個日益增長的威脅，其目的是藉由技術手段與資訊，影響目標族群思想與價值觀，從中製造認知暨情感上的衝突。至於被敵人視為目標的人力資本，將成為國家防禦中的一項弱點，因為大部分國家已經是高度相互連結與依賴開放系統，人的大腦易傾向於相信接收到的資訊為真實，較少主動懷疑或驗證；因此，容易受到錯誤資訊的影響。畢竟在人類歷史中，合作比懷疑更有助於生存，所以大腦傾向先相信、再懷疑，也並非時刻對所有資訊都保持警覺性；故這種特性帶來的風險不僅會影響國防安全，還會波及整個社會。再者，由於大腦運作原則是以生存為主，當個體接收訊息並解讀為威脅時，無

註1：François du Cluzel, Cognitive Warfare (Norfolk, VA: NATO Allied Command Transformation, 2021), p.6, https:// innovationhub-act.org/wp-content/uploads/2023/12/20210113_CW-Final-v2-.pdf. Emphasis in original，檢索日期：2025年7月15日。

論是真實存在或是覺知到，此時大腦的恐懼中樞便會被激活，執行功能區域會變得混亂，理性決策過程就會中斷。[2]

三、廣告商與媒體機構完全理解人類大腦的傾向，藉此刺激人的本能衝動，以利吸引消費者或民眾，並推銷產品。同樣地，美國的戰略競爭對手如俄羅斯與中共，渠等也利用人的這種本能反應來影響大眾的想法與價值觀，藉此混淆、分化及削弱一國政府運作與各項規劃流程。此外，大腦的本能衝動，再加上其自然發展與整合方式，讓我們容易掉入像是「確認偏誤」(Confirmation Bias)思維陷阱中。「確認偏誤」係指人們傾向於優先選擇支持已有信念和預設觀點的訊息，同時忽視或排斥與這些信念相矛盾的訊息。換句話說，在面對威脅時，人們往往會尋求可證實自身信念的資訊，即使之後再接收到更新且可靠的資訊，也難以改變他們原本想法。[3]

四、美國的戰略競爭對手(俄國與中共)深知，只要能在資訊空間中大量灌輸假訊息，人腦就容易信以為真，甚至會找理由來說服自己那是真的；也就是藉由人易於記憶的資訊、熟悉主題和片面真實內容來進行飽和攻勢，進而為新的敘事鋪路，造成潛移默化的影響。俄、「中」兩國正在將這種認知戰術納入軍事教戰守則之中，並動用國家權力工具與各種資源，針對美軍官兵與群眾發動各種大小不一的影響力行動，[4]這種戰術可歸類成「不對稱作戰」之一環，毋須動用傳統武器，僅藉由資訊操控與心理滲透，就能削弱對手軍心士氣與社會凝聚力。

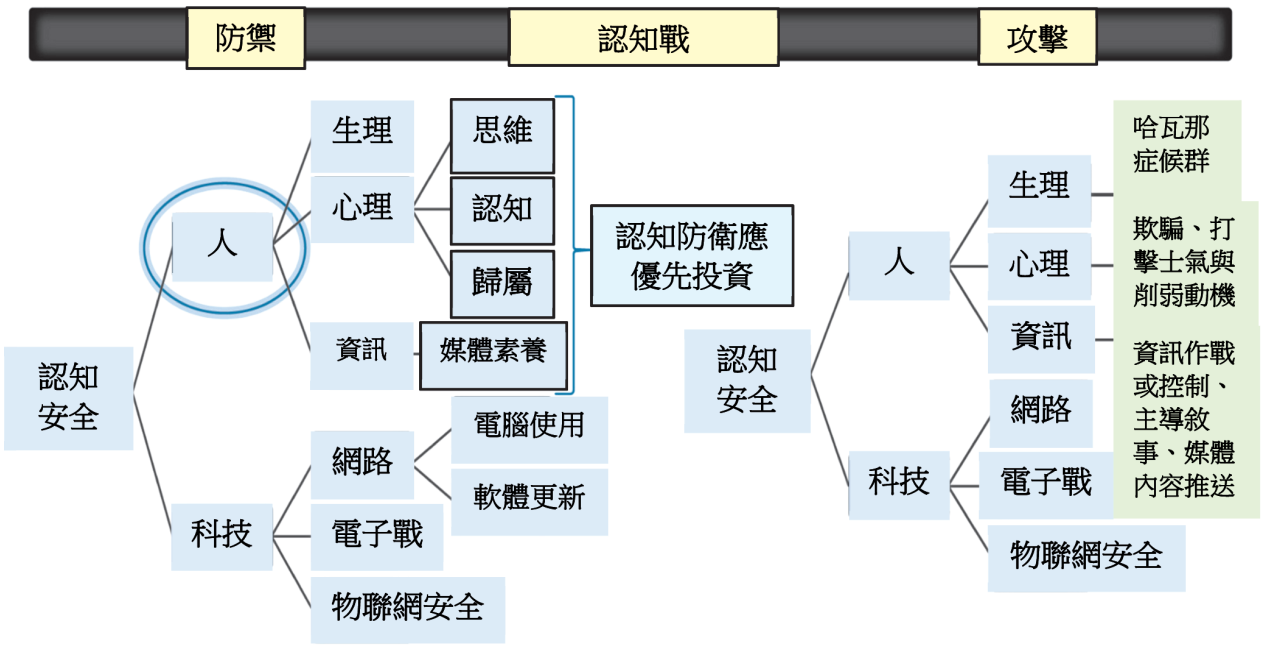
參、認知領域

一、美國國防部在發展適用於認知領域的「戰術、技術及程序」(Tactics, Techniques, and Procedures)時，必須思考該領域中涉及技術與人的面向，才能確保有效識別與防禦。在攻勢作為上，「美國網路司令部」(U.S. Cyber Command)就運用資訊作戰與心理作戰，持續在科技與人文領域中擴大部署；於此同時，國防部推動的資訊網路防禦作業和年度例行性網路安全訓練，則屬於守勢作為之一環。由於美軍目前尚未建立一個具體且有效應對的機制，以維護認知領域的安全，凸顯聯合部隊作戰仍存在缺口。畢竟攻擊與防禦構成「認知戰」的兩大要素，其中「科技

註2：Dave Grossman and Loren W. Christensen, On Combat: The Psychology and Physiology of Deadly Conflict in War and in Peace, 3rd ed. (Millstadt, IL: Warrior Science Publications, 2008), p.31; Alexis Artwohl, "Perceptual and Memory Distortion During Officer-Involved Shootings," FBI Law Enforcement Bulletin, Vol. 71, No. 10, October 2002, p.18, https://www.ojp.gov/ncjrs/virtual-library/abstracts/perceptual-and-memory-distortion-during-officer-involved-shootings，檢索日期：2025年7月16日。

註3：Daniel Kahneman, Thinking, Fast and Slow (New York: Farrar, Straus and Giroux, 2011), pp.80~81。

註4：Charles Cleveland et al., Military Strategy in the 21st Century: People, Connectivity, and Competition (Amherst, NY: Cambria Press, 2018), p.26。



圖一：「認知戰」的攻防示意圖

說明：「哈瓦那症候群」(Havana Syndrome)是指自2016年起，美國外交與情報人員在古巴首都哈瓦那及其他地點出現一系列不明原因的身體與認知症狀，如頭痛、暈眩、耳鳴、認知障礙及平衡障礙，至今成因仍具爭議，曾被懷疑與「定向能武器」(Directed Energy Weapon)或聲波攻擊有關，惟尚未有明確科學定論。

資料來源：參考 Michael J. Cheatham, Angelique M. Geyer, Priscella A. Nohle and Jonathan E. Vazquez, "Cognitive Warfare: The Fight for Gray Matter in the Digital Gray Zone," Joint Force Quarterly, No. 114, 3rd Quarter 2024, p.85，由譯者製圖。

」與「人」則各自內嵌其中(如圖一)，防禦機制必須全面融入各類軍事行動中，且無論時間、地點或作戰狀態為何，都不容忽視。

二、保護軍事人員的認知空間，對於美國維持相對戰略優勢至關重要，在認知安全中，關於人的心理與資訊防線是當前急需建立，如此才能以主動或被動防禦方式，讓美軍官兵避免受「認知戰」的影響。雖然科技依然是資訊與網路領域中傳遞訊息與防守能力的主要著力點，但美軍「聯合部隊」指揮官必須將「人的認知」列為優先事項，因為「認知戰」正是透過資訊與網路領域發揮其對人的影響力，況且在高度相互連結的作戰環境中，任何作戰領域都不可能「單打獨鬥」。

肆、美軍認知戰的對手

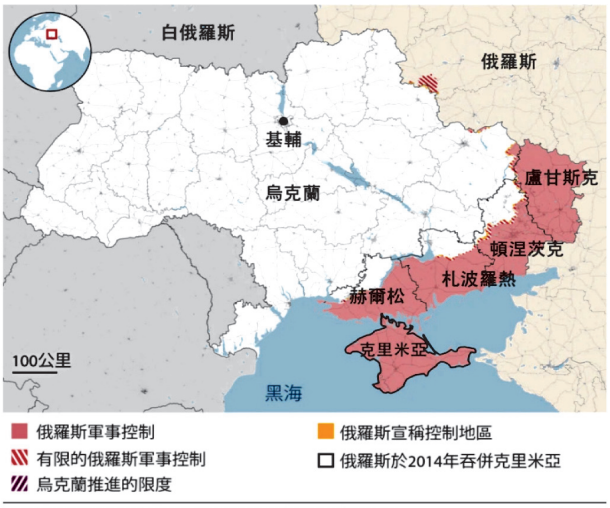
如今戰略競爭方式與過去已有所不同，曾經以爭奪主導地位與軍備優勢為主軸的「冷戰」，早已劃下句點。在傳統戰爭上，美國仍舊保持相對戰略優勢，俄羅斯與中共若堅決對美國進行常規作戰，不僅落敗風險極高，傷亡可謂慘重；鑑此，做

為較為可行的應對措施，俄、「中」就一直企圖操控目標族群中屬於柔性的道德因素，藉由獲取細微的進展，逐步在時間與空間中推動她們的行動。影響群眾如何解讀全球事件的發展，成為操控群眾反應行為的第一步，於此同時，也逐步推動自身想要達成的目標。

一、俄羅斯

(一)俄國認知作戰策略被稱為「反身控制」(Reflexive Control)，係一種通過影響對方認知過程來改變其決策的戰術。根據俄國的軍事理論指出，「反身控制」可從戰術層面一直應用到戰略層面。隨著科技與通訊速度的提升，該策略的潛在威力也逐漸擴大；再加上在過去30年間，俄方還持續運用名為「馬斯基洛夫卡」(Maskirovka，意指欺敵/偽裝)的伎倆，透過假訊息操作來捏造資訊與形塑公眾認知，進而在群眾中引發混亂反應。[5]至於「馬斯基洛夫卡」乙詞可追溯至沙皇俄國時期的萌芽，並在蘇聯紅軍時代達成系統化運用。

(二)俄方發動的假訊息戰旨在避免動用實體軍事行動，同時藉由掩蓋行動來源的策略，以假冒美國組織或是個人在資訊與網路領域中的活動，[6]這種可歸類為「灰色地帶」(Gray Zone)的軍事行動方式，刻意模糊俄國與西方對戰爭定義的界線。那些將戰爭狹隘定義成以武力或實體行動為主的西方國家，必須理解這種觀點其實是自我設限，一旦被這種框架限制住，民主國家不但無法真正瞭解敵人，而且也無法真正瞭解自己，誠如《孫子兵法》所言，「知己知彼，百戰不殆；不知彼而知己，一勝一負；不知彼，不知己，每戰必殆。」



圖二：俄國在克里米亞與烏克蘭的控制區

資料來源：參考保羅・柯比(Paul Kirby)，〈澤倫斯基為何不能、也不會放棄克里米亞？〉，BBC中文，2025年4月25日，https://www.bbc.com/zhongwen/articles/cgkg03v0pk7o/trad，檢索日期：2025年7月18日，由譯者綜整製圖。

(三)在2016年美國總統大選期間，由於俄方認為川普(Donald Trump)當選將有

註5：Timothy Thomas, "Russia's Reflexive Control Theory and the Military," The Journal of Slavic Military Studies, Vol. 17, No. 2, 2004, p.239。

註6：Scott Shane, "The Fake Americans Russia Created to Influence the Election," New York Times, September 7, 2017, https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html，檢索日期2025年7月15日。

表一：中共信息對抗體系表

信　息　攻　擊	項目	信　息　防　禦
雷達、通信、電磁與光學干擾、導航及水中聲波干擾。	電子	電子隱蔽、電子欺騙、發射源聯網。
邊界滲透、網路控制、指揮中樞攻擊、欺敵攻擊、病毒破壞。	網路	防病毒攻擊、防駭客攻擊、網路復原、防止電磁洩露、網路使用管理。
心理宣傳誘導、心理嚇阻、心理操控、心理欺騙。	心理	心理動機、心理調適、心理韌性、心理衛生照護。
反輻射飛彈攻擊、定向能武器攻擊、火力打擊與特種干擾。	資訊設施	建立防破壞機制。

資料來源：參考Jeffrey Engstrom, Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare, RR-1708-OSD, RAND Corporation, February 2018, p.67，由譯者綜整製表。

利於改善雙邊關係，所以採取多項支持川普的行動，此舉不僅干預了民主國家的自由選舉，更可視為一場針對民主國家及其公民的現代「認知戰」，且具有高度指標性與深遠的戰略意涵。[7]俄國攻擊方式是利用言論自由的理念來破壞美國大選的程序，在臉書(Facebook)、X(前身為推特【Twitter】)、YouTube等社群媒體平臺，散播關於競選對手希拉蕊(Hillary Clinton)的虛假資訊，藉此削弱選舉過程的公正性。此外，俄國在2014年入侵克里米亞與2022年入侵烏克蘭行動之前(如圖二)，俄羅斯總統普丁(Vladimir Putin)也擴大對全球受眾的假訊息宣傳，企圖為其行動正當性辯護。[8]俄方還利用國營廣播機構向外界傳播虛假敘事，扭曲西方民眾對這些事件的正常理解。[9]

二、中共

(一)中共將「認知戰」歸類在「信息對抗體系」中，該體系將心理活動跟網路、電子及資訊系統攻擊，並列視為同等重要的手段(如表一)，另輔以宣傳、威懾、影響與欺騙等手法。[10]至於「認知戰」是架構在「三戰」(輿論戰、心理戰、法律戰)的基礎上，也就是「認知戰」是「三戰」的延伸。「中」、俄雙方一樣，將戰爭視為是一種持續的競爭狀態，透過運用所有國家力量工具來實現其目標。美國國

註7：Media Ajir and Bethany Vailliant, "Russian Information Warfare: Implications for Deterrence Theory," Strategic Studies Quarterly, Vol. 12, No. 3, Fall 2018, pp.70-89, https://www.airuniversity.af.edu/portals/10/ssq/documents/ volume-12_issue-3/ssqfall2018.pdf，檢索日期：2025年7月17日。

註8：Lennart Maschmeyer, "Digital Disinformation: Evidence from Ukraine," Center for Security Studies Analyses in Security Policy, No. 278, February 2021, p.4, https://doi. org/10.3929/ethz-b-000463741，檢索日期：2025年7月18日。

註9：Erik C. Nisbet and Olga Kamenchuk, "The Psychology of State-Sponsored Disinformation Campaigns and Implications for Public Diplomacy," The Hague Journal of Diplomacy, Vol. 14, No. 1-2, April 2019, pp.65-82, https://brill.com/view/journals/hjd/14/1-2/article-p65_6.xml，檢索日期：2025年7月19日。

註10：Nathan Beauchamp-Mustafaga, Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States, RRA853-1, RAND Corporation, June 2023, pp.39,129, https://www.rand.org/content/dam/rand/pubs/research_reports/ RRA800/RRA853-1/RAND_RRA853-1.pdf，檢索日期：2025年7月20日。

防部與美軍官兵應提高警覺並強化辨識能力，才能揪出惡意行為，像是網路數據竊取、選舉干預，以及其他旨在影響認知空間的攻擊行動。[11]

(二)在軍事規劃中，瞭解人們對空間組織與利益分布的認知方式，與理解地形如何影響行軍與部署同樣關鍵。這就是所謂的「人文地理繪製」(Human Geography Mapping)，係指運用地圖、圖資或資料視覺化的方式，描繪、分析並呈現人類活動與空間分布的關係，此一能力具備潛在的核心作戰價值，值得進一步的研究與分析。據瞭解，中共已將這個概念納入軍事準則之中，「心理偵察」(Psychological Reconnaissance)能夠用來評估心理作戰對不同人群的影響，[12]其為中共整體偵察情報系統的一部分，該系統亦涵蓋電子與網路偵察。[13]共軍在進行攻防行動的同時，也會評估部隊的心理動機、維護心理健康、培養面對壓力環境的耐力，以及在必要時提供心理創傷的即時照護。

(三)防禦認知領域的攻擊是共軍在「信息對抗體系」中的關鍵部分，相較之下，美軍並未將認知領域的防禦納入其作戰體系之中，反而是將之視為單獨的醫療支援回應來處理。此外，中共對外的戰略競爭手段還融合西方的作戰方式，涵蓋資訊、政治及經濟層面的混合行動。[14]這種手段導致戰場範圍模糊、態勢持續又不斷演化，進一步複雜化美軍的防禦作為與應對能力。面對中共這種認知戰的部署，「認知防禦」(Cognitive Defense)自應成為美軍聯合部隊每位成員都應具備的基本技能(俄、「中」兩國對認知戰內涵比較，如表二)。

伍、數位灰色地帶(Digital Gray Zone)

一、「數位灰色地帶」是指介於和平與戰爭、合法與非法之間，在數位與網路空間中進行的模糊性影響行動，該地帶已成為「認知戰」的實踐空間與操作場域。「物聯網」(Internet of Things)的興起再加上資訊獲取速度變快，就算是不太使

註11：Tzu-Chieh Hung and Tzu-Wei Hung, "How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars," Journal of Global Security Studies, Vol. 7, No. 4, June 2020, pp.1~18, https://doi. org/10.1093/jogss/ogac016，檢索日期：2025年7月20日。

註12：Jeffrey Engstrom, Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare, RR-1708-OSD, RAND Corporation, February 2018, pp.86~89, https:// www.rand.org/pubs/research_reports/ RR1708.html，檢索日期：2025年7月21日。

註13：同前註。

註14：Geoffrey Parker, ed., The Cambridge History of Warfare (New York: Cambridge University Press, 2005), pp.1-11; Michael J. Mazarr, Bryan Frederick, and Yvonne K. Crane, Understanding a New Era of Strategic Competition, RRA290-4, RAND Corporation, November 2022, pp.6~7, https://www.rand.org/content/ dam/rand/pubs/research_reports/RRA200/ RRA290-4/RAND_RRA290-4.pdf.，檢索日期：2025年7月22日。

表二：俄羅斯與中共對「認知戰」內涵彙整表

分類	俄　羅　斯	中　　共
體系	「認知戰」屬「混合戰」的一環。	「認知戰」屬信息對抗體系的一環，是「三戰」(輿論、心理、法律)的延伸。
策略	反身控制：透過操縱敵方對現實的理解，進而引導其行動，也就是讓敵人按我方所望方式思考與行動。	「三戰」由中共軍事科學院提出並於2003年納入共軍政工條例。 ●輿論戰：操作媒體、新聞、社群媒體、內容農場及運用網軍干預。 ●心理戰：恫嚇、煽動、瓦解對方士氣，削弱民心或破壞社會穩定。 ●法律戰：為中共的政治或軍事行動建立法理正當性，爭奪國際法與話語權詮釋的主導權。
操作手法	●高度依賴匿名網軍、低成本技術、偏向破壞性應用、非制度化的訊息操作。 ●法律與教育並非俄國「認知戰」的主力工具，較偏重心理操作與社會情緒引爆。 ●借用AI生成、「深偽」(Deepfake)技術、大數據分析、社群演算法操控。	●依賴國家體系主導、法律與媒體結合的系統性操作手法。 ●對南海、臺灣等議題，透過法理敘事來建構行動正當性，另透過文教、學術機構來進行文化性認知滲透。 ●借用AI生成、「深偽」(Deepfake)技術、大數據分析、社群演算法操控。
案例	●2014年併吞克里米亞行動。 ●2016年干預美國總統大選。 ●2022年俄、烏戰爭爆發前後的訊息操作。	●長期對臺軍事威嚇與和平統一敘事。 ●2016年南海仲裁案後的國際法理戰與敘事操作。 ●2020年「新冠肺炎」(COVID-19)疫情起源反擊的敘事。

資料來源：參考張玲玲，〈強化精神戰力，反制認知作戰〉，《青年日報》，2024年6月20日，https://www.ydn.com.tw/news/newsInsidePage?chapterID=1686009；董慧明，〈建立全方位社會韌性，反制認知作戰操弄〉，《青年日報》，2025年5月23日，https://www.ydn.com.tw/news/newsInsidePage?chapterID=1767802，檢索日期：2025年7月22日，由譯者自行製表。

用科技的人，也早已被數位世界深深包圍。「數位沉浸」(Digital Immersion)進一步改變人們處理資訊的方式，閱讀行為從傳統的線性邏輯轉變為快速瀏覽，無論各種來源資訊是真是假，都被人們快速掃過，只要標題具吸引力，可能就被誤認為是事實。[15]

二、如今，人們普遍透過標題與社群媒體來尋求「快速資訊片段」(Quick Hits)，但這種行為對閱聽者構成重大風險，俄、「中」兩國正好看準這點，有意識地利用這種趨勢擴大其影響力。「錯誤資訊片段」(Disinformation Bits)無論是在第一時間的感知層面，或是在有意識與無意識的處理過程中，皆為刻意散布與操控的結果，這無疑對聯合作戰構成獨特挑戰，並在個人層面形成難以預測的威脅。

三、2020年，46歲的非裔美國人喬治・佛洛伊德(George Floyd)之死為「數位灰色地帶」戰術的運用案例，事件發生在美國明尼蘇達州明尼亞波利斯市(Minneapolis)，該員因涉嫌使用假鈔被捕時，

註15：Nicholas Carr, The Shallows: What the Internet Is Doing to Our Brains (New York: W.W. Norton and Company, 2011), p.9。

遭警察跪壓脖頸處超過8分鐘，致其失去知覺，送醫後宣告死亡。其後與該事件相關的大量社群媒體貼文，源頭都可追溯至俄國與中共帳號，[16]這些由國家支持的貼文，背後都隱藏著精心算計，意在激化美國國內群眾的情緒反應。假訊息與情緒煽動的相互結合，並對準美國戰略敘事的核心，形成一種非傳統但極具效果的打擊方式。

四、「敘事空間」(Narrative Space)是民主制度政府的一個戰略重心，其是讓一個國家能實現所望目標的力量或權力來源，這對美國而言至關重要。[17]由於俄羅斯與中共在現階段不太可能在傳統軍事上打敗美國，並取得決定性勝利；它們轉而採取一種策略，旨在對美國造成「功能性失敗」(Functional Defeat)，這不是要征服領土或摧毀軍事力量，而是要摧毀支持抵抗意志的道德因素。在民主制度中，民意是權力的驅動力，當社會大眾的心中逐漸被混亂與不信任籠罩時，民主體制內的權力平衡就會開始動搖。此時，敵我雙方的意識形態對抗，即使不動用武力，也可能藉由輿論與心理影響，改變原本勢均力敵的戰略局勢。

陸、大腦的灰質地帶

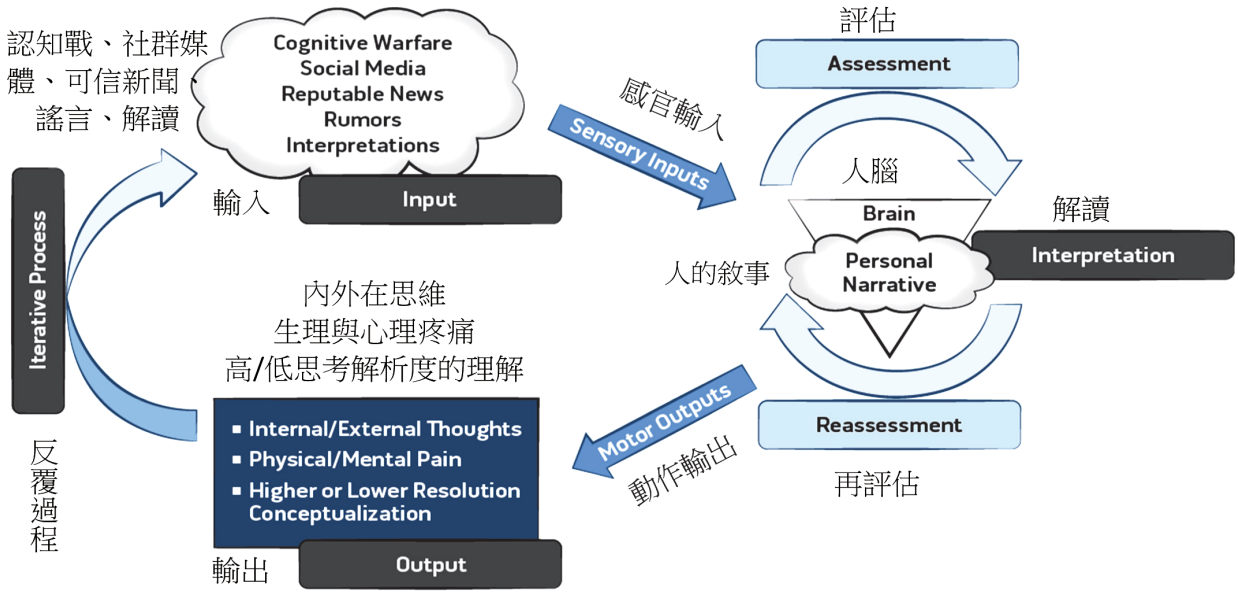
一、人類大腦是以神經序列性與反覆循環的方式運作，其過程是經由輸入、解讀，再到輸出所組成的迴圈(如圖三)。[18]在這樣的運作迴圈下，有助於人們強化對外界的預測性與確定感，進而提升生存機率；然而假訊息會讓人陷入「低解析度」(Low-Resolution)的理解狀態，也就是模糊人們對環境現況與應對策略的認知，形成資訊模糊、錯誤反應、認知失真。當不確定性進入人的大腦運作迴圈(即輸入、解讀、輸出)的過程時，大腦會試著尋找更多資訊，以填補資訊落差並進行交叉驗證；而「確認偏誤」就容易從中產生，也是人們傾向只接收與原本想法一致的資訊，形成一個錯誤資訊的迴圈，不斷加深錯誤的觀念。

二、人們透過經驗、信念、自我反思，以及他人對自己的看法來建構個人敘事時，只要錯誤資訊滲透入內在信念，將會阻礙個人所處時空的「心理地圖」(Mental Map)，個人敘事就容易受到影響並發生改變。接著「低解析度的心理地圖」顯示出對生存的認知威脅，進而啟動大腦的

註16：Mark Scott, “Russia and China Target U.S. Protests on Social Media,” Politico, June 1, 2020, http://politico.eu/article/russia-china-us-protests-social-media-twitter/，檢索日期：2025年7月23日。譯者註：兩份驗屍報告確認佛洛伊德死亡為「他殺」：第一份是2020年6月1日，亨內平郡(Hennepin County)法醫報告指出，死因為「執法壓頸及制伏引起的心肺停止」；第二份是家屬委託的第二份驗屍則強調「因頸部與背部壓迫導致窒息」。2021年4月20日，過失警察遭判定犯有二級過失殺人、三級謀殺與二級過失致死；6月25日，他被判刑22年半。

註17：Joint Publication 5-0, Joint Planning (Washington, DC: The Joint Staff, December 2020), pp. IV~22。

註18：W. Eric Cobb, Z-Health R-Phase Certification Manual, 5th ed. (Tempe, AZ: Z-Health Performance Solutions, 2013), p.5。



圖三：人的敘事處理過程示意圖

說明：圖中評估、再評估的反覆循環，對於形塑人的敘事處理過程至關重要。

資料來源：參考Michael J. Cheatham, "Cognitive Warfare: The Fight for Gray Matter in the Digital Gray Zone," Joint Force Quarterly, No. 114, 3rd Quarter 2024, p.88，由譯者翻譯製圖。

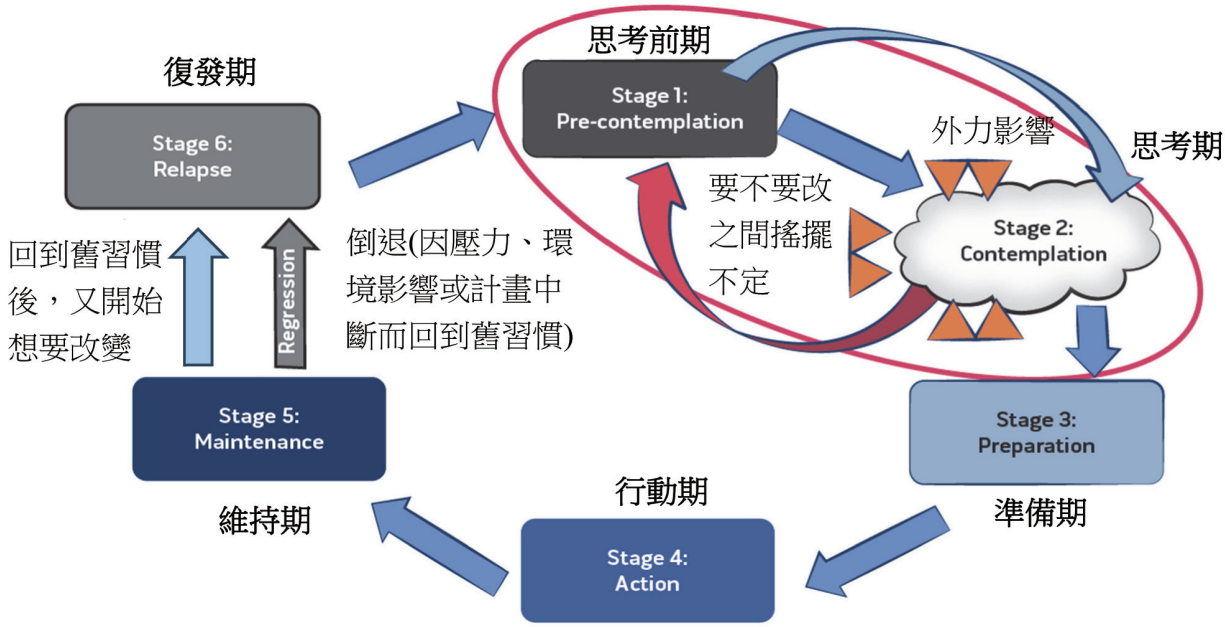
壓力系統，形成高度警覺模式；因此，長時間接觸錯誤資訊與持續的高度警覺，可能扭曲個人的自我認知與存在結構。對於「認知戰」問題缺乏理解或過於天真無知，將使個體容易產生認知失調，這種失調可能會出現各種無法預期的表現，例如憤怒、幻滅(對原本相信的事物失望)、虛無主義(覺得一切毫無意義)，甚至自我傷害。[19]

柒、改變始於覺知

一、發展「認知戰」反制作為至關重要，前提在於我們必須先有基本的覺知，也就是意識到問題的存在，唯有覺知才能改變。「行為的變化階段模型」(Stages of Change Model)主張，要將個體從當前的行為狀態轉變為所望狀態，必須經歷包含思考前期(Pre-Contemplation)、思考期(Contemplation)、準備期(Preparation)、行動期(Action)、維持期(Maintenance)、復發期(Relapse)等六個階段。[20]循環週期間強調，在「認知戰」中要改變一個人的想法，前兩個階段最為重要(如圖四)。「思考前期」為個人尚未意識到自己需要

註19：Jordan B. Peterson, 12 Rules for Life: An Antidote to Chaos (Toronto: Random House Canada, 2018), p.87。

註20：Karen Glanz and Barbara K. Rimer, Theory at a Glance: A Guide for Health Promotion Practice (Bethesda, MD: National Cancer Institute, 1997), pp.17~18。



圖四：行為的變化階段示意圖

資料來源：參考Michael J. Cheatham, "Cognitive Warfare: The Fight for Gray Matter in the Digital Gray Zone," Joint Force Quarterly, No. 114, 3rd Quarter 2024, p.89，由譯者翻譯製圖。

改變，也沒有要改變的打算；「思考期」為個人開始意識到問題的存在，並在思考是否要改變。

二、由於個體的自我意識與對改變的抗拒，往往限制組織系統可以改變的幅度。在當前「認知戰」的環境中，聯合部隊的許多官兵仍處於「思考前期」，也就是尚未意識到有改變的必要；在這個階段，個人與組織不是尚未意識到問題的存在，也就是不承認該問題需要採取策略性應對。總的來說，渠等尚未準備好進行改變。[21]唯有清楚去定義問題，提升官兵對問題的認知，才能有助於從「思考前期」轉變至「思考期」。

三、當個人與組織意識到問題存在，開始思考採取行動的步驟時，就進入「思考期」，[22]這個階段是一個著手思考並規劃行動的過程，其關鍵在於個人或組織如何解讀及改變這件事，若改變的觀念受到過多外在壓力，將引發一種潛在威脅感，這會讓個人或組織為尋求確定性、可預測性及生存感，導致退回到不願意面對改變的狀態。因此，個人或組織必須從內部著手推動改變的觀念，改變的驅動力量，必須符合個人或組織的敘事與信念，以利讓每個成員都能內化對當前「認知戰」正在

註21：Jason M. Satterfield, Mind-Body Medicine: The New Science of Optimal Health (Chantilly VA: The Teaching Company, 2013), p.25。

註22：同註21。

發生的理解，並從中意識到自身正面臨的風險。唯有發展超越基本生存層級的思考與操作能力，持續讓大腦執行功能區域參與資訊處理，才能在面對「認知戰」時，擁有更強的心理韌性與判斷力。

捌、美國反制認知戰的因應之道

認知安全必須從具備基本韌性開始，這種韌性表現在「明辨是非」，研究指出，具有高度政治意識與數位素養的個人，其在面對以敘事為主的「認知戰」時，心理上較難被滲透，[23]原因在於這些人辨別事實的能力較強，較能準確識破錯誤資訊，較不會產生一些負面情緒或反應。換言之，健全的心理防護，並將認知安全的概念推廣至美軍聯合部隊，係因應「認知戰」的重要一步。認知安全的戰略策訂有三項行動主軸，說明如后：

一、高層重視、強化官兵教育及排定周期性訓練

(一)美國國防部應責成「聯合參謀部」(Joint Staff)研議，將「認知戰」納入作戰領域，成為繼陸、海、空、太空、網路五大作戰領域後的另一個作戰領域；而且在「認知戰」中，大腦思維是最為關鍵且脆弱的攻擊目標，能掌控並主導對方的認知能力，正是美軍所追求之戰果。不僅如此，美軍還應將網軍、電子戰、資訊支援等整合為一個「認知作戰領域」(Cognitive Warfighting Domain)，才能促使領導高層優先配置資源，以強化對該領域競爭情勢的重視。國防部必須理解科技與資訊作戰如何影響個人在消化資料及做決策時的認知能力，同時將認知韌性視為一種無形的武器系統來加以發展。

(二)國防部應在各層級的軍事訓練中納入「認知戰」課程，從基礎訓練至專業軍事教育各階段，因材施教，並列入部隊基地的年度例行驗證項目。透過教育訓練讓官兵認識訊息如何塑造思維模式，以及「確認偏誤」對決策過程的影響。此外，領導者應主動教育官兵，告知科技科技發展、社群媒體所引發「近因偏誤」(Recency Bias)與「社交仿冒」(Social Spoofing)對決策過程產生之影響，說明如后：

1.「近因偏誤」是指人在做判斷或決策時，過度重視最近接收到的資訊，反而忽略過去的重要資訊或整體趨勢。「認知戰」的運用是大量推播特定事件的最新消息，讓目標群體高估事件影響，以產生恐慌、焦慮或情緒反應，進而影響社會決策或民意走向。舉例而言，在「俄烏戰爭」期間，俄國媒體散播烏國當局在頓巴斯

註23：Amy Mitchell et al., Distinguishing Between Factual and Opinion Statements in the News (Washington, DC: Pew Research Center, 2018), p.3, https://www.csus.edu/indiv/f/friedman/fa2019/govt1/schedule/a/fact-opinion. pdf.，檢索日期：2025年7月24日。

(Donbas)地區不當暴行的假影片(如圖五)。儘管後來經查證這段影片其實是剪輯合成的假訊息，來源為俄方操作的帳號，但許多民眾卻在第一時間就已經相信此一虛假訊息。

2.「社交仿冒」是指為融入某個社群或符合群體期待，刻意模仿並迎合他人的行為與想法；在「認知戰」的運用上是惡意操作者偽裝成可信賴的社交對象、意見領袖或群體成員，以從事資訊操縱或影響目標受眾的認知。舉例而言，俄羅斯支持的行動者曾建立一系列假帳號，冒充「北約」軍官、外交官或軍事分析人士，在「X」(推特)、「領英」(LinkedIn)和「臉書」等平臺上活動，目的是進行滲透軍事與政策圈社群、散播錯誤訊息與分化言論，以誘導真實人員與之互動。

(三)鑑此，領導幹部應致力於強化官兵的媒體識讀能力、認知重評技巧學習，以及各項促進歸屬感與部隊凝聚力的活動，以強化防禦當前的認知攻擊事件。美國國防部亦應指導各軍種將「認知戰」的防禦機制納入現有的心理韌性計畫之中，以預先強化官兵的認知與心理素質，進而提升渠等在面對認知攻擊時的抵抗力。[24]最後，與其依賴高學歷、持有專業證照的心理健康專家來主導訓練，還不如由經專業培訓的戰術層級領導者來擔任師資；至於在戰術層級的綜合訓練，能讓訓練更靈活、成本更低，以及提升官兵對訓練的投入與認同。[25]

圖五：俄國媒體散播烏國當局不當暴行的假影片

資料來源：參考劉宗翰譯，〈「俄烏戰爭」前的俄羅斯「影響力行動」〉，《海軍學術雙月刊》(臺北市)，第57卷，第1期，2023年2月1日，頁132。

二、強化媒體素養

(一)當資訊環境被大量虛假訊息充斥時，易使人產生「資訊學習無助感」，也就是覺得再怎麼判斷資訊也無法分辨真假，會產生無力感或放棄辨識；[26]至於以被動方式攻擊那些本身已有憂鬱、低自尊與悲觀傾向的官兵，往往最具效果。最新研究顯示，美軍人員約有一成五屬於這類高風險群體，[27]為了防範此類攻擊，領導幹部亦應強化媒體素養訓練計畫，以提升官

註24：J. Malekos Smith, “The Best Natural Defense to Psychological Warfare,” Small Wars Journal, December 25, 2016, https://smallwarsjournal.com/jrnl/art/the-best-natural-defense-to-psychological-warfare，檢索日期：2025年7月26日。

註25：同註24。

註26：同註9。

兵的推理判斷與資訊解讀能力。

（二）美國著名智庫「蘭德公司」（RAND）、非營利國際組織「國際研究與交流委員會」（IREX）與「哈佛大學」（Harvard University）的研究結果顯示，官兵若能先期接受媒體素養影片與相關訓練，將有效降低假訊息散播風險，顯著減弱敵操控資訊的影響力。[28]這些公開研究可讓大家理解現有資訊與教育資源的研究發現，意識到問題的嚴重性，強調培養媒體素養之重要性。至於媒體素養教材可從現有民間資源中獲得，例如在佛羅里達州的教育系統正推行的「Cyber Florida」計畫[29]，相關訓練也應透過正式與非正式的持續性計畫，以及各個軍事支援組織來推動。唯有強化媒體素養，才能提升官兵在媒體環境中的自信與判別真假資訊的能力。[30]

三、發展防禦機制

（一）技術可用以協助識別假訊息的傳播模式，甚至追踪出那些試圖操控特定訊息的來源；[31]同理，美國國防部可運用「人工智慧」（AI）與「機器學習」（ML）技術來發展防禦工具，協助軍事領導層打擊敵企圖在公共論壇散布假訊息的行動。舉例而言，可透過運用AI技術進行自動化的「機器人偵測」或「機器人標記」，以辨識社群媒體中散播假訊息的假帳號。[32]人工智慧亦可做為教育輔助工具，藉由揭示敵假訊息的操控行為，教導防範與應對技巧，以降低未來受影響的風險。[33]

（二）美國華府智庫「戰略暨國際研究中心」（CSIS）高級助理史密斯（Zhanna Malekos Smith）建議，可運用技術來發展防禦機制，以協助資訊處理、模式識別及來源追溯。[34]就宏觀面來看，「人工智慧」與「機器學習」有助於在高度資訊氾濫

註27：Shannon L. Exley and Lindsay M. Oberman, “Repetitive Transcranial Magnetic Stimulation for the Treatment of Depression, Post-Traumatic Stress Disorder, and Suicidal Ideation in Military Populations: A Scholarly Review,” Military Medicine Vol. 187, No. 1-2, January-February 2022, p.73, https://doi. org/10.1093/milmed/usab187. 檢索日期：2025年7月28日。

註28：Peter W. Singer and Eric B. Johnson, “The Need to Inoculate Military Servicemembers Against Information Threats: The Case for Digital Literacy Training for the Force,” War on the Rocks, February 1, 2021, http://warontherocks.com/2021/02/we-need-to-inoculate-militaryservicemembers-against-information-threats-the-case-for-digital-literacy-training/，檢索日期：2025年8月4日。

註29：譯者註：該計畫是佛羅里達州政府與「南佛羅里達大學」(South Florida University)合作成立的綜合性資安平臺，整合從基礎至高階的教育訓練、跟學界及產業共同推動的研發與政策倡議，以及應用於公部門與社區的實務資安推廣。“Cyber Florida, Florida Center for Instructional Technology, and New America Launch New Partnership to Improve ‘Cyber Citizenship’ Skills for K-12 Students,” New America, December 16, 2020, https://www.newamerica.org/international-security/press-releases/cyber-florida-fcit-new-america-partnership-to-improve-cyber-citizenship/，檢索日期：2025年8月5日。

註30：“Randomized Control Trial Finds IREX’ s Media Literacy Messages to Be Effective in Reducing Engagement With Disinformation,” IREX, October 20, 2020, https://www.irex.org/news/randomized-control-trial-finds-irexs-media-literacy-messages-be-effective-reducing-engagement，檢索日期：2025年8月6日。

註31：同註28。

註32：Linda Slapakova, “Towards an AI-Based Counter-Disinformation Framework,” The RAND Blog, March 29, 2021, https://www.rand.org/blog/2021/03/towards-an-ai-based-counterdisinformation-framework.html，檢索日期：2025年8月8日。

註33：同註32。

的環境中辨識出模式。誠如史密斯引述的諺語：「謊言已傳遍全球，真相卻還在穿鞋(A Lie Can Travel Halfway Around the World while the Truth Is Still Putting on Its Shoes)」[35]這句諺語提醒我們一個關於假訊息的普遍事實，又再次強調決策者長期以來所面對的挑戰；除了眼前的這項挑戰外，另一個挑戰是當前資訊傳遞之規模龐大與高速流動，已遠超出大多數人在整合、分析並理解海量資訊的能力範圍。

玖、結論

一、美國國防部必須優先關注當前資訊環境會誤導官兵認知的風險，並理解美軍普遍缺乏應對此挑戰所需的教育、技能與反制認知的能力。在「認知戰」中，即便是微小事件亦可能產生累積的心理效應，進而削弱人的思考能力及做出可能挑戰原有價值觀的決策。此外，國防部還必須同步推動相關措施，以防止聯合部隊遭受散播不當意圖之假訊息攻擊。領導者應界定問題，運用或發展反制策略，以培養個人主動識別並對抗假訊息的能力。

二、「認知戰」威脅的存在需要獲得充分承認，才能有助於制定中和或反制認知攻擊的策略。領導者也必須採取具體的後續平衡作為，才能讓聯合部隊因應當前與未來挑戰；因此，理解人的層面為關鍵弱點，將有助於發展保護認知領域的攻防行動。唯有積極採取行動，強化並優化認知防禦之戰力，才能為聯合部隊鋪設轉型之路，從傳統消耗戰邁入即將展開之「認知戰」新紀元。[36]

三、美軍各軍種若能妥善運用教育訓練，強化官兵意識並落實標準作業流程，將有助於維持強大敘事的作戰重心，確保韌性達到應有的標準。這類課程應要求全體官兵在初階訓練、季度訓練及年度訓練期間接受認知技能強化磨練，同時將相關內容納入專業軍事教育體系。為防止平民遭受「認知戰」攻擊，也應採取預防性策略；反之，若僅依賴事後反應來應對「認知戰」，不僅流程繁瑣、成本高昂，而且成效也有限。

四、應發展一套適用於軍事人員及廣泛群體的認知防禦架構，將直接或間接強化美軍的心理韌性。畢竟隨著俄羅斯與中共將「認知戰」視為優先戰術選項，美軍面對的相關風險將進一步攀升；由此亦可見，美軍領導高層必須將認知防禦納為國防部的核心能力之一。

註34：同註24。
註35：同註24。
註36：Megan Friedl, “Goldfein Delivers Air Force Update,” U.S. Air Force, September 19, 2017, https://www.af.mil/News/Article-Display/Article/1316603/goldfein-delivers-air-force-update/，檢索日期：2025年8月10日。

拾、譯後語

「認知戰」為一場沒有煙硝味的戰爭，其破壞力不亞於傳統武力衝突，這是一種不依賴傳統軍事手段，而是針對人的認知與決策機制進行操控與干擾的戰爭形式，目的在削弱對手意志、干擾判斷、引發內部混亂，進而達成戰略或政治之目的。「數位灰色地帶」正成為現代衝突的前線，它無聲無形、界限模糊，可以在不發一槍一彈情況下，癱瘓對手的信任系統與社會穩定；因此，理解並建立相關防禦策略與韌性，已是民主國家未來將面對的關鍵課題。

我國已身處在「認知戰」的前線，特別是來自中共持續發動的認知攻擊，根據我國「國家安全局」指出，2024年觀察到的爭議訊息數量共計215萬9,000則，超過2023年總量132萬9,000則，兩年內呈現穩定上升趨勢，至於2025年前四個月就達51萬餘則，近期中共甚至針對「台積電赴美投資」等議題，運用官媒、自媒體、網軍組織及公關公司，配合異常帳號帶風向、駭客偽冒發文及操控代理人帳號等，企圖操弄輿論、分化社會共識，進而削弱我國內部穩定與民眾信任，[37]其發展確實值得注意。

我國確實需要對「數位灰色地帶」有更深刻的瞭解，並儘速研擬應對之法，本文所提因應之道的建議，應該可提供國軍或政府部門列入參考；至於「認知戰」反制作為亦應多樣化，才能應對中共施展的各種手段。[38]總體而論，我國若能在認知領域建立有效因應模式，其成功經驗不僅可供其他受威脅的民主國家參考，還能有機會成為全球民主陣營在防禦「認知戰」上的先鋒，進一步強化民主聯盟反制極權國家認知滲透的整體能力。 ⚓

作者簡介：

美空軍中校麥可・奇塔姆(Michael J. Cheatham)為美國國防部聯合參謀部安全辦公室副主任。

安潔莉克・蓋耶(Angelique M. Geyer)為美國海岸防衛隊隊長兼大西洋區作戰規劃組組長。

美陸軍中校普莉希拉・諾爾(Priscella A. Nohle)為「北約盟軍轉型司令部」未來作戰戰略官。

美空軍中校強納森・瓦茲奎茲(Jonathan E. Vazquez)為美國國防部聯合參謀部情報副署長轄下的情報蒐集管理科科長，兼任亞太地區首席情報蒐集協調官。

譯者簡介：

劉宗翰中校，國防大學管理學院93年班、政治大學外交系戰略所碩士104年班。曾任排長、《國防譯粹月刊》主編，現服務於國防部政務辦公室暨軍事譯著主編。

註37：吳書緯，〈中共散布爭議訊息今年已逾51萬則，國安局曝認知戰路徑〉，中央通訊社，2025年4月8日，https://www.cna.com.tw/news/aipl/202504080109.aspx，檢索日期：2025年8月11日。

註38：曾雅琦，〈「後疫情時代」中共對臺「認知作戰」威脅淺析〉，《海軍學術雙月刊》(臺北市)，第56卷，第4期，2022年8月1日，頁135。